Avira Free Antivirus

Manuale utente

Marchio registrato e copyright

Marchio registrato

Windows è un marchio registrato di Microsoft Corporation negli Stati Uniti e in altri paesi.
Tutti gli altri marchi o nomi di prodotti sono marchi registrati del legittimo proprietario.
I marchi protetti non sono contrassegnati come tali in questo manuale. Ciò tuttavia non significa che possano essere liberamente utilizzati.

Note sul Copyright

Per Avira Free Antivirus viene utilizzato il codice di terzi. Ringraziamo i possessori di copyright per aver messo a disposizione il proprio codice.
Informazioni dettagliate sul copyright sono disponibili nella Guida in linea di Avira Free Antivirus in "Third Party Licenses".

Indice

1. Introduzione

Il prodotto Avira in uso permette di proteggere il computer da virus, worm, trojan, adware e spyware e altri rischi. In breve, in questa guida si parla di virus, malware (software dannosi) e programmi indesiderati.

La guida descrive l'installazione e il funzionamento del programma.

Sul nostro sito Web sono disponibili diverse opzioni e ulteriori informazioni:

http://www.avira.it

Sul sito Web di Avira è possibile:

- visualizzare informazioni relative ad altri programmi Avira per il desktop
- scaricare i programmi Avira per il desktop più recenti
- scaricare le guide del prodotto più recenti in formato PDF
- scaricare tool gratuiti per l'assistenza e la riparazione
- accedere alla completa Knowledge Base e alle domande frequenti per la risoluzione dei problemi
- visualizzare gli indirizzi dell'assistenza specifici per ogni paese.

Il team di Avira

1.1 Simboli ed evidenziazioni

Vengono utilizzati i seguenti simboli:

Simbolo/Definizione	Spiegazione
✓	Indica un requisito che deve essere soddisfatto prima che sia eseguita un'operazione.
▸	Indica un'operazione da eseguire.
↳	Indica un evento scaturito dall'operazione precedente.
Avviso	Indica un avviso di pericolo di una significativa perdita di dati.

Nota	Indica un messaggio con informazioni particolarmente importanti o un suggerimento che agevola la comprensione e l'uso del prodotto Avira.

Vengono utilizzate le seguenti evidenziazioni:

Evidenziazione	Spiegazione
Corsivo	Nome del file o percorso.
	Elementi dell'interfaccia software che vengono visualizzati (ad esempio sezione della finestra o messaggio di errore).
Grassetto	Elementi dell'interfaccia software su cui è possibile fare clic (ad es. voci di menu, rubriche, campi di opzione o pulsanti).

2. Informazioni sul prodotto

In questo capitolo è possibile consultare tutte le informazioni rilevanti per l'acquisto o l'utilizzo del prodotto Avira:

- vedere capitolo: Prestazioni
- vedere capitolo: Requisiti di sistema
- vedere capitolo: Licenza e aggiornamento

I prodotti Avira offrono tool completi e flessibili per garantire una protezione affidabile del computer da virus, malware, programmi indesiderati e altri pericoli.

- Nota:

Avviso
La perdita di dati importanti ha spesso conseguenze drammatiche. Nemmeno il miglior programma antivirus può offrire una protezione al 100% contro la perdita di dati. Si consiglia di eseguire regolarmente copie di sicurezza (backup) dei dati.

Nota
Un programma in grado di proteggere il computer da virus, malware, programmi indesiderati e altri pericoli può essere affidabile ed efficace solo se aggiornato regolarmente. Si consiglia di garantire l'aggiornamento del prodotto Avira con gli aggiornamenti automatici. Configurare il programma in modo adeguato.

2.1 Prestazioni

Il prodotto Avira in uso offre le seguenti funzionalità:

- Control Center per il monitoraggio, l'amministrazione e la gestione dell'intero programma
- Configurazione centrale con configurazione semplice in modalità esperto oppure standard e dotata di guida in linea sensibile al contesto
- System Scanner (On-Demand Scan) con scansione di tutti i tipi noti di virus e malware gestita dal profilo e configurabile
- Integrazione nella funzionalità di controllo di Windows Vista (Controllo dell'account utente) per poter eseguire operazioni per le quali sono necessari i diritti di amministratore.
- Real-Time Protection (On-Access Scan) per il costante monitoraggio di tutti gli accessi ai file

- Avira SearchFree Toolbar, una barra di ricerca integrata nel browser Web per ricerche rapide e comode su Internet. La toolbar contiene anche i widget delle funzioni più importanti per la navigazione su Internet.
- Web Protection (per gli utenti di Avira Free Antivirus solo abbinata ad Avira SearchFree Toolbar) per il controllo di dati e file provenienti da Internet tramite il protocollo HTTP (controllo delle porte 80, 8080, 3128)
- Avira Free Android Security è un'app che protegge i dispositivi da furto e/o smarrimento. L'app comprende funzioni che consentono di individuare il dispositivo portatile quando è stato messo chissà dove oppure, peggio ancora, in caso di furto. Quest'applicazione permette inoltre di bloccare le telefonate o gli SMS in arrivo. Avira Free Android Security protegge i telefoni cellulari e gli smartphone basati sul sistema operativo Android.
- Gestione integrata della quarantena per l'isolamento e il trattamento di file sospetti
- Rootkits Protection per l'individuazione di malware installati e nascosti nel sistema del computer (i cosiddetti rootkit) (non disponibile per Windows XP a 64 bit)
- Accesso diretto in Internet a informazioni dettagliate su virus rilevati e malware
- Aggiornamento semplice e rapido del programma, dei file delle definizioni dei virus (VDF) e del motore di ricerca tramite aggiornamento di file singolo e aggiornamento VDF incrementale mediante un server Web su Internet
- Pianificatore integrato per la pianificazione di operazioni singole o ricorrenti come aggiornamenti o scansioni
- Identificazione estremamente precisa di virus e malware per mezzo di tecnologie di ricerca (motore di ricerca) che includono la procedura di ricerca euristica
- Identificazione di tutti i tipi di archivio convenzionali, inclusa l'identificazione di archivi nascosti e Smart-Extension
- Prestazioni elevate grazie alla capacità multi threading (scansione contemporanea di molti file ad alta velocità)

2.2 Requisiti di sistema

Sussistono i seguenti requisiti di sistema:

- Computer a partire dal Pentium, minimo 1 GHz
- Sistema operativo
  - Windows XP, SP più recente (a 32 o 64 bit) oppure
  - Windows Vista, SP più recente (a 32 o 64 bit) oppure
  - Windows 7, SP più recente (a 32 o 64 Bit)

> **Nota**
> Tenere presente che per ora il nostro software non è compatibile con Windows 8.

- Almeno 150 MB di memoria libera sull'hard disk (maggiore quantità di memoria se si utilizza la quarantena e la memoria temporanea)
- Almeno 512 MB di memoria di lavoro in Windows XP
- Almeno 1024 MB di memoria di lavoro in Windows Vista, Windows 7
- Per l'installazione del programma: diritti di amministratore
- Per tutte le installazioni: Windows Internet Explorer 6.0 o superiore
- Eventuale connessione Internet (vedere Installazione)

Avira SearchFree Toolbar

- Sistema operativo
  - Windows XP, SP più recente (a 32 o 64 bit) oppure
  - Windows Vista, SP più recente (a 32 o 64 bit) oppure
  - Windows 7, SP più recente (a 32 o 64 Bit)
- Browser Web
  - Windows Internet Explorer 6.0 o superiore
  - Mozilla Firefox 3.0 o superiore
  - Google Chrome 18.0 o superiore

> **Nota**
> Eventualmente disinstallare le barre di scansione già installate prima dell'installazione di Avira SearchFree Toolbar, altrimenti non è possibile installare Avira SearchFree Toolbar.

Note per gli utenti di Windows Vista

In Windows XP molti utenti lavorano con i diritti di amministratore. Tuttavia questo non è auspicabile dal punto di vista della sicurezza, poiché così anche i virus e i programmi indesiderati hanno la possibilità di infiltrarsi nel computer.

Per questo motivo, Microsoft con Windows Vista ha introdotto il controllo utente (Controllo dell'account utente). Questa funzione protegge maggiormente gli utenti registrati come amministratore, perché l'amministratore dispone in Windows Vista inizialmente solo dei privilegi di un utente normale. Le azioni per le quali sono necessari i diritti di amministratore sono chiaramente segnalate da Windows Vista con un'icona. Inoltre l'utente deve esplicitamente confermare l'azione desiderata. Dopo aver ricevuto l'approvazione, si registra un aumento dei privilegi e il sistema operativo esegue i propri compiti amministrativi.

Il prodotto Avira necessita dei diritti di amministratore per eseguire alcune azioni in Windows Vista. Queste azioni sono contrassegnate dal seguente carattere: . Se questo carattere appare su un pulsante, significa che sono necessari i diritti di amministratore per

l'esecuzione di tale azione. Se l'attuale utente non dispone di tali diritti, Windows Vista propone una finestra di dialogo del Controllo Utente (Controllo dell'account utente) per l'inserimento della password dell'amministratore. Se non si dispone di tale password, non è possibile eseguire questa azione.

2.3 Licenza e aggiornamento

Per poter utilizzare il prodotto Avira è necessario possedere una licenza. È necessario accettare le condizioni di licenza.

La licenza viene assegnata mediante una chiave di licenza digitale in forma di file *.KEY*. Questa chiave di licenza digitale è il fulcro dei comandi della propria licenza personale. Contiene indicazioni precise su quali programmi hanno la licenza e per quale periodo. Una chiave di licenza digitale può anche contenere una licenza per più prodotti.

La chiave di licenza digitale viene comunicata in un'e-mail se il prodotto Avira è stato acquistato su Internet oppure si trova sul CD o DVD del programma.

3. Installazione e disinstallazione

In questo capitolo sono disponibili informazioni relative all'installazione e alla disinstallazione del prodotto Avira:

- vedere capitolo: Prima dell'installazione: Requisiti, preparazione del computer per l'installazione
- vedere capitolo: Installazione rapida: Installazione standard con le impostazioni predefinite
- vedere capitolo: Installazione personalizzata: Installazione configurabile
- vedere capitolo: Assistente di configurazione
- vedere capitolo: Modifica dell'installazione
- vedere capitolo: Moduli di installazione
- vedere capitolo: Disinstallazione: Esecuzione della disinstallazione

3.1 Tipi di installazione

Durante l'installazione mediante l'assistente di installazione è possibile selezionare un tipo di setup:

Express

- I file del programma vengono installati in una directory standard predefinita in *C:\Programmi*.
- Il prodotto Avira viene installato con le impostazioni standard. È possibile stabilire le impostazioni predefinite nell'assistente di configurazione.

Personalizzato

- Con l'installazione personalizzata è possibile selezionare singoli componenti del programma (vedere capitolo Installazione e disinstallazione > Moduli di installazione).
- Si può scegliere una cartella di destinazione per i file di programma da installare.
- È possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu di avvio.
- Con la configurazione guidata è possibile effettuare impostazioni personalizzate del prodotto Avira e indurre una breve scansione del sistema direttamente dopo l'installazione.

3.2 Prima dell'installazione

> **Nota**
> Prima dell'installazione verificare che il computer risponda ai requisiti di sistema. Se il computer soddisfa tutti i requisiti è possibile installare il prodotto Avira.

> **Nota**
> Nell'installazione su un sistema operativo server, Real-Time Protection e Protezione file non sono disponibili.

Inizializzazione prima dell'installazione

✓ Chiudere il programma e-mail. Si consiglia inoltre di chiudere tutte le applicazioni in uso.

✓ Assicurarsi che non siano installate altre protezioni contro virus. Le funzioni automatiche di protezione di diverse applicazioni antivirus potrebbero entrare in conflitto.

↳ Il prodotto Avira scansionerà il computer per controllare l'eventuale presenza di software incompatibili.

↳ In caso di rilevamento di software incompatibile viene generato un elenco corrispondete di questi programmi.

↳ Si consiglia di disinstallare il software che espone a rischi la sicurezza del computer.

- Scegliere dall'elenco quei programmi, che devono essere eliminati dal computer automaticamente, quindi fare clic su **Avanti**.
- Alcuni programmi possono essere eliminati dal computer solo manualmente. Selezionare i programmi e fare clic su **Avanti**.

↳ La disinstallazione di uno o più programmi richiede il riavvio del computer. Dopo il riavvio, l'installazione continua.

> **Avviso**
> Finché la procedura di installazione del prodotto Avira non è conclusa, il computer non è protetto.

Installazione

Il programma di installazione funziona in modalità di dialogo. Nella maggior parte dei passaggi di installazione è sufficiente fare un semplice clic per continuare.

I pulsanti principali hanno le seguenti funzioni:

- **OK**: conferma l'operazione.
- **Annulla**: annulla l'operazione.
- **Avanti**: passa alla fase successiva.
- **Indietro**: passa alla fase precedente.

▶ Stabilire una connessione a Internet. La connessione a Internet è necessaria per eseguire i seguenti passaggi dell'installazione:

- Scaricare i file attuali di programma e del motore di ricerca, nonché i file di definizione dei virus aggiornati mediante il programma di installazione (per installazione basata su Internet)
- Aggiornare, se necessario, a installazione conclusa

> Nota
> **Installazione basata su Internet:**
> per eseguire un'installazione basata su Internet del programma è disponibile un programma di installazione che carica i file di programma attuali prima di eseguire l'installazione dai server Web di Avira. Tale procedura garantisce l'installazione del prodotto Avira con un file di definizione dei virus aggiornato.
>
> **Installazione con un pacchetto di installazione:**
> il pacchetto di installazione contiene sia il programma di installazione sia tutti i file di programma necessari. Nell'installazione con un pacchetto di installazione non è possibile effettuare la selezione della lingua per il prodotto Avira. Al termine dell'installazione si consiglia di eseguire un aggiornamento del file di definizione dei virus.

3.3 Installazione Express

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

↳ Appare la finestra di dialogo **Benvenuti**.

▶ Fare clic su **Avanti** per continuare l'installazione.

↳ Appare la finestra di dialogo **Seleziona lingua**.

▶ Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Installazione con un pacchetto di installazione

↳ Viene visualizzata la finestra **Preparazione dell'installazione in corso**.

↳ Il file di installazione viene decompresso. La routine di installazione viene avviata.

↳ Appare la finestra di dialogo **Selezionare modalità di installazione**.

> **Nota**
> L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è impostata come predefinita. Se si desidera eseguire un'**Installazione personalizzata**, continuare a leggere qui di seguito: Installazione > Installazione personalizzata.

- Confermare **l'accettazione della licenza utente finale**. Se si desidera leggere i dettagli dei contratti di licenza, fare clic sul link relativo.
- Fare clic su **Avanti**.

  ↳ Viene visualizzata la finestra di dialogo **Si unisca ai milioni di utenti Avira che già utilizzano Avira SearchFree**.

- Se non si desidera installare Avira SearchFree Toolbar, cancellare il contrassegno dalla casella di Avira SearchFree Toolbar e Avira SearchFree Updater **Accettazione della licenza** e disattivare l'impostazione di **Avira SearchFree (search.avira.com)** come pagina iniziale.

> **Nota**
> Eventualmente disinstallare le barre di scansione già installate prima dell'installazione di Avira SearchFree Toolbar, altrimenti non è possibile installare Avira SearchFree Toolbar.

- Fare clic su **Avanti**.

  ↳ L'*assistente per l'installazione della licenza* si apre e aiuta l'utente nell'attivazione del programma.

  ↳ A questo punto è possibile configurare un server proxy.

  ↳ L'avanzamento dell'installazione viene indicato da una barra verde.

  ↳ Fare clic su **Fine** per terminare il setup e uscire dal programma di installazione.

  ↳ L'Icona Tray di Avira si trova nella barra delle applicazioni.

  ↳ Il modulo **Updater** ricerca gli eventuali aggiornamenti disponibili per proteggere in modo ottimale il computer.

↳ La finestra di stato **Luke Filewalker** si apre con una prima ricerca diretta del sistema di scansione e informa l'utente circa lo stato della scansione visualizzandone i risultati.

- Se dopo la scansione del sistema viene richiesto di riavviare il sistema, eseguire tale operazione per consentire la protezione completa del sistema stesso.

3.4 Installazione personalizzata

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

↳ Appare la finestra di dialogo **Benvenuti**.

- Fare clic su **Avanti** per continuare l'installazione.

↳ Appare la finestra di dialogo **Seleziona lingua**.

- Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Installazione con un pacchetto di installazione

↳ Viene visualizzata la finestra **Preparazione dell'installazione in corso**.

↳ Il file di installazione viene decompresso. La routine di installazione viene avviata.

↳ Appare la finestra di dialogo **Selezionare modalità di installazione**.

> **Nota**
> L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è impostata come predefinita. Se si desidera eseguire tale operazione, continuare a leggere qui di seguito: Installazione > Installazione Express.

- Come modalità di installazione desiderata selezionare **Personalizzata**.
- Confermare **l'accettazione della licenza utente finale**. Se si desidera leggere i dettagli dei contratti di licenza, fare clic sul link relativo.
- Fare clic su **Avanti**.

↳ Viene visualizzata la finestra di dialogo **Si unisca ai milioni di utenti Avira che già utilizzano Avira SearchFree**.

- Se non si desidera installare Avira SearchFree Toolbar, cancellare il contrassegno dalla casella di Avira SearchFree Toolbar e Avira SearchFree Updater **Accettazione della licenza** e disattivare l'impostazione di **Avira SearchFree (search.avira.com)** come pagina iniziale.

> **Nota**
> Eventualmente disinstallare le barre di scansione già installate prima dell'installazione di Avira SearchFree Toolbar, altrimenti non è possibile installare Avira SearchFree Toolbar.

- Fare clic su **Avanti**.

  ↳ Appare la finestra **Selezionare directory di destinazione**.

  ↳ Da directory predefinita è *C:\Programmi\Avira\AntiVir Desktop*

- Fare clic su **Avanti** per continuare l'installazione.

  - OPPURE -

  Selezionare con **Sfoglia** un'altra directory di destinazione e confermare con **Avanti**.

  ↳ Appare la finestra **Installa componenti**.

- Attivare o disattivare i componenti desiderati e confermare con **Avanti**.
- Nelle seguenti finestre di dialogo è possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu.
- Fare clic su **Avanti**.
- Dopo la chiusura del processo di installazione, terminare quest'ultima con **Fine**.

  ↳ Si chiude l'assistente di installazione e si apre l'assistente di configurazione.

3.5 Assistente di configurazione

Al termine dell'installazione personalizzata si apre l'assistente di configurazione. Nell'assistente di configurazione è possibile configurare impostazioni importanti per il prodotto Avira in uso.

- Fare clic su **Avanti** nella finestra di benvenuto dell'assistente di configurazione per iniziare la configurazione del programma.

  ↳ Nella finestra di dialogo **Configura AHeAD** è possibile selezionare un livello di riconoscimento per la tecnologia AHeAD. Il livello di riconoscimento selezionato viene registrato per l'impostazione della tecnologia AHeAD di System Scanner (scansione diretta) e di Real-Time Protection (scansione in tempo reale).

- Selezionare un livello di riconoscimento e proseguire la configurazione con **Avanti**.

↳ Nella finestra di dialogo seguente **Seleziona categorie estese delle minacce** è possibile adattare le funzioni di protezione del prodotto Avira con la selezione delle categorie delle minacce.

- Attivare eventualmente ulteriori categorie delle minacce e proseguire la configurazione con **Avanti**.

↳ Nel caso in cui si sia selezionato il modulo di installazione Avira Real-Time Protection, appare la finestra di dialogo **Modalità di avvio di Real-Time Protection**. È ora possibile stabilire il momento in cui avviare Real-Time Protection. Real-Time Protection viene avviato nella modalità di avvio a ogni riavvio del computer.

Nota
La modalità di avvio indicata di Real-Time Protection viene memorizzata nel registro e non può essere modificata mediante la configurazione.

Nota
Al momento dell'avvio del computer, un'eventuale conseguenza della selezione della modalità di avvio di default per Real-Time Protection (avvio normale) e di un rapido accesso all'account utente può essere la mancata scansione dei programmi che si avviano automaticamente all'avvio del sistema, dal momento che essi vengono avviati prima del completo caricamento di Real-Time Protection.

- Attivare l'opzione desiderata e proseguire la configurazione con **Avanti**.

↳ Nella finestra di dialogo seguente **Scansione del sistema** è possibile attivare o disattivare l'esecuzione di una scansione rapida del sistema. La scansione rapida del sistema viene eseguita al termine della configurazione e prima di riavviare il computer, e verifica la presenza di virus e malware nei programmi avviati e nei file di sistema più importanti.

- Attivare o disattivare l'opzione **Scansione rapida del sistema** e proseguire la configurazione con **Avanti**.

↳ Nella finestra di dialogo seguente è possibile terminare la configurazione con **Fine**.

↳ Le impostazioni indicate e selezionate vengono registrate.

↳ Se è attivata l'opzione **Scansione rapida del sistema** si apre la finestra **Luke Filewalker**. System Scanner esegue una scansione rapida del sistema.

↳ Se dopo la scansione del sistema viene richiesto di riavviare il sistema, eseguire tale operazione per consentire la protezione completa del sistema stesso.

Se l'installazione è avvenuta con successo, si consiglia di verificare lo stato di aggiornamento del programma di protezione nella sezione **Stato** del Control Center.

- Se il prodotto Avira visualizza un messaggio ad indicare che il computer non è completamente protetto, fare clic su **Risoluzione del problema**.
  - ↳ Verrà visualizzata la finestra di dialogo **Ripristina la protezione**.
- Massimizzare la sicurezza del sistema in uso attivando le opzioni prestabilite.
- Infine, è possibile eventualmente eseguire una scansione completa del sistema.

3.6 Modifiche all'installazione

È possibile aggiungere o rimuovere singoli componenti del programma all'attuale installazione del prodotto Avira (vedere capitolo Installazione e disinstallazione > Moduli di installazione)

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **Pannello di controllo** di Windows.

Selezionare il prodotto Avira e fare clic su **Cambia**. Nella finestra di dialogo di benvenuto del programma, selezionare l'opzione **Modifica programma**. Si è così inseriti nella modifica dell'installazione.

> **Nota**
> Quando si disinstalla Avira SearchFree Toolbar, viene disinstallato anche Web Protection.

3.7 Moduli di installazione

Nel caso di un'installazione personalizzata o di una modifica di un'installazione è possibile selezionare, aggiungere o eliminare i seguenti moduli:

- **Avira Free Antivirus**
  Questo modulo contiene tutti i componenti necessari per l'installazione corretta del prodotto Avira.
- **Real-Time Protection**
  Real-Time Protection viene eseguito in background. Monitora e ripara i file, quando possibile, durante operazioni come apertura, scrittura e copia in tempo reale (On-Access = all'accesso). Se un utente esegue un'operazione (caricamento, esecuzione, copia di un file), il prodotto Avira scansiona automaticamente il file. Durante l'operazione di rinomina del file, Real-Time Protection di Avira non esegue alcuna scansione.
- **Rootkits Protection**
  Avira Rootkits Protection controlla se sul computer sono già installati software che dopo l'intrusione nel computer non si riesce a rilevare con i metodi convenzionali del riconoscimento di malware.

- **Web Protection** (per gli utenti di Avira Free Antivirus solo insieme a Avira SearchFree Toolbar)
  Quando si naviga su Internet, mediante il browser Web i dati vengono recuperati da un server Web. I dati trasferiti dal server Web (file HTML, file di script e immagini, file flash, file audio e video, ecc.) normalmente passano dalla cache del browser direttamente all'esecuzione nel browser Web cosicché non è possibile una scansione in tempo reale così come messa a disposizione da Avira Real-Time Protection. In questo modo virus e programmi indesiderati potrebbero entrare nel computer. Web Protection è un cosiddetto proxy HTTP che monitora le porte utilizzate per il trasferimento dei dati (80, 8080, 3128) e controlla la presenza di virus e programmi indesiderati nei file trasferiti. In base alla configurazione, il programma tratta i file infetti automaticamente o chiede all'utente l'azione da eseguire.
- **Shell Extension**
  Le estensioni Shell creano nel menu contestuale di Esplora risorse di Windows (tasto destro del mouse) la voce *Controlla i file selezionati con Avira.* Con questa voce è possibile scansionare direttamente singoli file o directory.

3.8 Disinstallazione

Se si desidera eliminare il prodotto Avira dal proprio computer, è possibile utilizzare l'opzione **Cambia/Rimuovi programmi** di **Installazione applicazioni** nel Pannello di controllo di Windows.

È possibile disinstallare il prodotto Avira (descritto ad esempio per Windows 7) nel seguente modo:

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.
- Fare doppio clic su **Programmi e funzionalità**.
- Selezionare il prodotto Avira dall'elenco e fare clic su **Disinstalla**.
  - ↳ Verrà chiesto all'utente se desidera davvero eliminare il programma.
- Confermare con **Sì**.
  - ↳ Tutti i componenti del programma vengono eliminati.
- Fare clic su **Fine** per terminare la disinstallazione.
  - ↳ Appare una finestra di dialogo con il suggerimento di riavviare il computer.
- Confermare con **Sì**.
  - ↳ Il prodotto Avira viene quindi disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

Nota
L'Avira SearchFree Toolbar non viene disinstallata con il programma, ma deve essere infatti disinstallata separatamente tramite i suddetti passaggi. Per fare

questo è necessario attivare l'Avira SearchFree Toolbar tramite l'Add-On Manager. Al termine della disinstallazione, la barra di ricerca non è più integrata nel browser.

Nota
Quando si disinstalla Avira SearchFree Toolbar, viene disinstallato anche Web Protection.

4. Panoramica di Avira Free Antivirus

In questo capitolo è possibile consultare una panoramica delle funzionalità e del funzionamento del prodotto Avira.

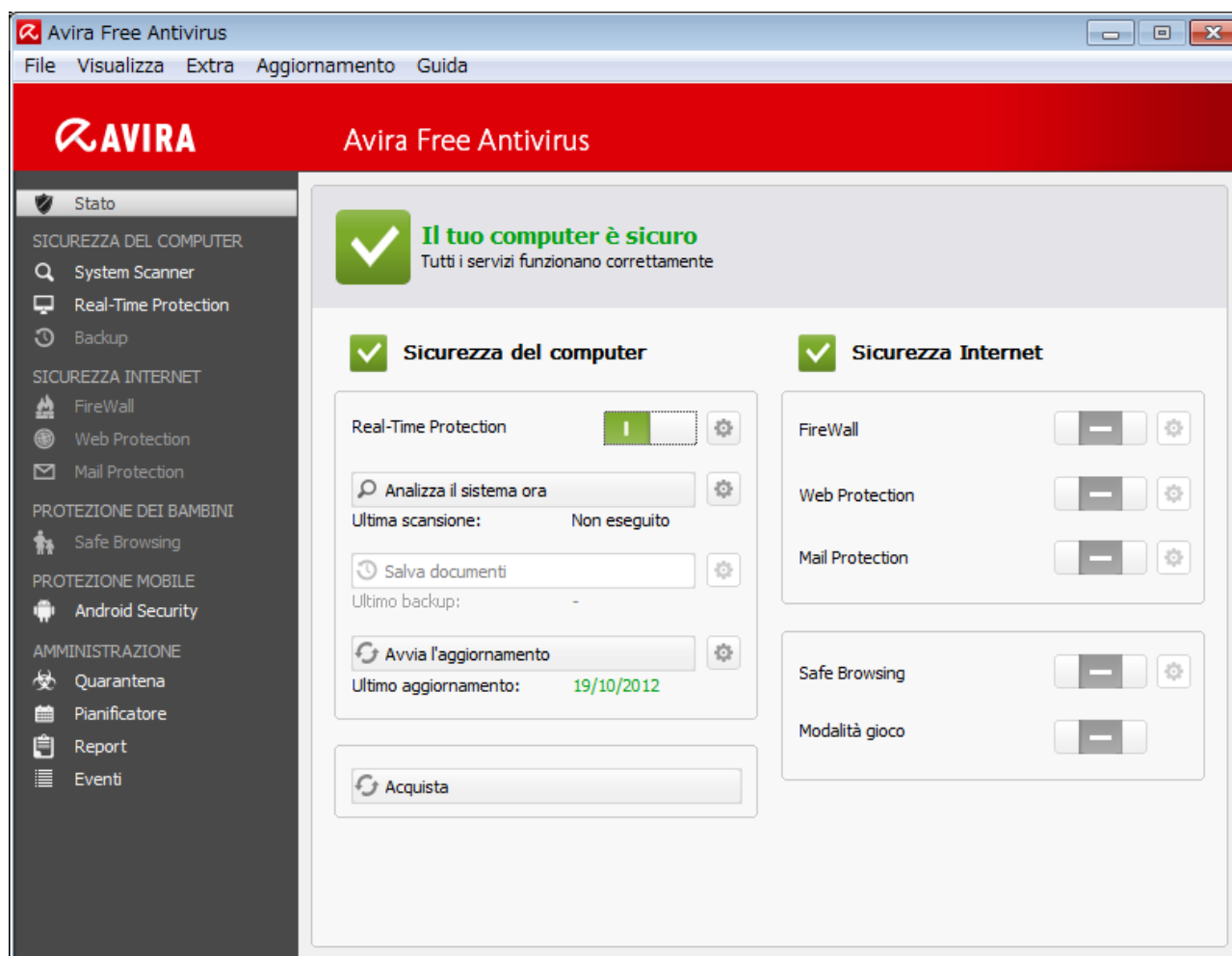
- vedere capitolo Interfaccia e funzionamento
- vedere capitolo Avira SearchFree Toolbar
- vedere capitolo Come procedere

4.1 Interfaccia utente e funzionamento

È possibile usare il prodotto Avira mediante tre elementi dell'interfaccia del programma:

- Control Center: monitoraggio e gestione del prodotto Avira
- Configurazione: configurazione del prodotto Avira
- Icona Tray nella barra delle applicazioni: apertura di Control Center e altre funzioni

4.1.1 Control Center

Control Center serve per il monitoraggio dello stato di protezione del computer e per la gestione e il funzionamento dei componenti di protezione e delle funzioni del prodotto Avira in uso.

La finestra di Control Center è suddivisa in tre aree: la **barra dei menu**, l'**area di navigazione** e la finestra dettagliata **Stato**:

- **Barra dei menu:** nei menu di Control Center è possibile richiamare funzioni generali del programma e informazioni sul prodotto.
- **Area di navigazione:** nell'area di navigazione è possibile passare in modo semplice da una rubrica all'altra di Control Center. Le singole rubriche contengono informazioni e funzioni dei componenti del programma e sono presenti sulla barra di navigazione in base alle sezioni dei task. Esempio: sezione dei task *SICUREZZA DEL COMPUTER* - Rubrica **Real-Time Protection**.
- **Stato:** nella schermata iniziale **Stato** viene mostrato se il computer è sufficientemente protetto, quali moduli sono attivi e quando sono stati eseguiti l'ultimo backup e l'ultima scansione del sistema. Nella finestra **Stato** sono presenti i pulsanti per l'esecuzione di funzioni e operazioni, ad esempio l'attivazione o disattivazione di **Real-Time Protection**.

Avvio e chiusura di Control Center

Per avviare Control Center è possibile scegliere tra le seguenti modalità:

- Fare doppio clic sull'icona del programma sul desktop

- Mediante la voce del programma nel menu **Start > Programmi**.
- Mediante l'icona Tray del prodotto Avira.

Si può chiudere Control Center mediante il comando **Chiudi** nel menu **File**, con la combinazione di tasti **Alt+F4** o facendo clic sulla x nella finestra di Control Center.

Utilizzo di Control Center

Come navigare in Control Center:

- Fare clic sulla barra di navigazione su un'area del task sotto la rubrica.
  - ↳ La sezione dei task viene visualizzata con ulteriori possibilità di funzione e di configurazione nella finestra dettagliata.
- Eventualmente fare clic su un'altra sezione dei task per visualizzarla nella finestra dettagliata.

> **Nota**
> Attivare la navigazione da tastiera nella barra dei menu con l'ausilio del tasto [**Alt**]. Con il tasto **Invio** si attiva la voce di menu selezionata in quel momento. Per aprire, chiudere o navigare nei menu di Control Center è possibile utilizzare anche le combinazioni di tasti [**Alt**] + carattere sottolineato nel menu o comando. Tenere premuto il tasto [**Alt**] se si desidera richiamare dal menu un comando o un sottomenu.

Come elaborare dati o oggetti che vengono visualizzati nella finestra dei dettagli:

- Evidenziare i dati o gli oggetti che si desidera elaborare.

  Per evidenziare più elementi, tenere premuto il tasto **Ctrl** o il tasto **Maiusc** (selezione di elementi consecutivi) durante la selezione degli elementi.
- Fare clic sui pulsanti desiderati nella barra superiore della finestra dei dettagli per elaborare l'oggetto.

Control Center in sintesi

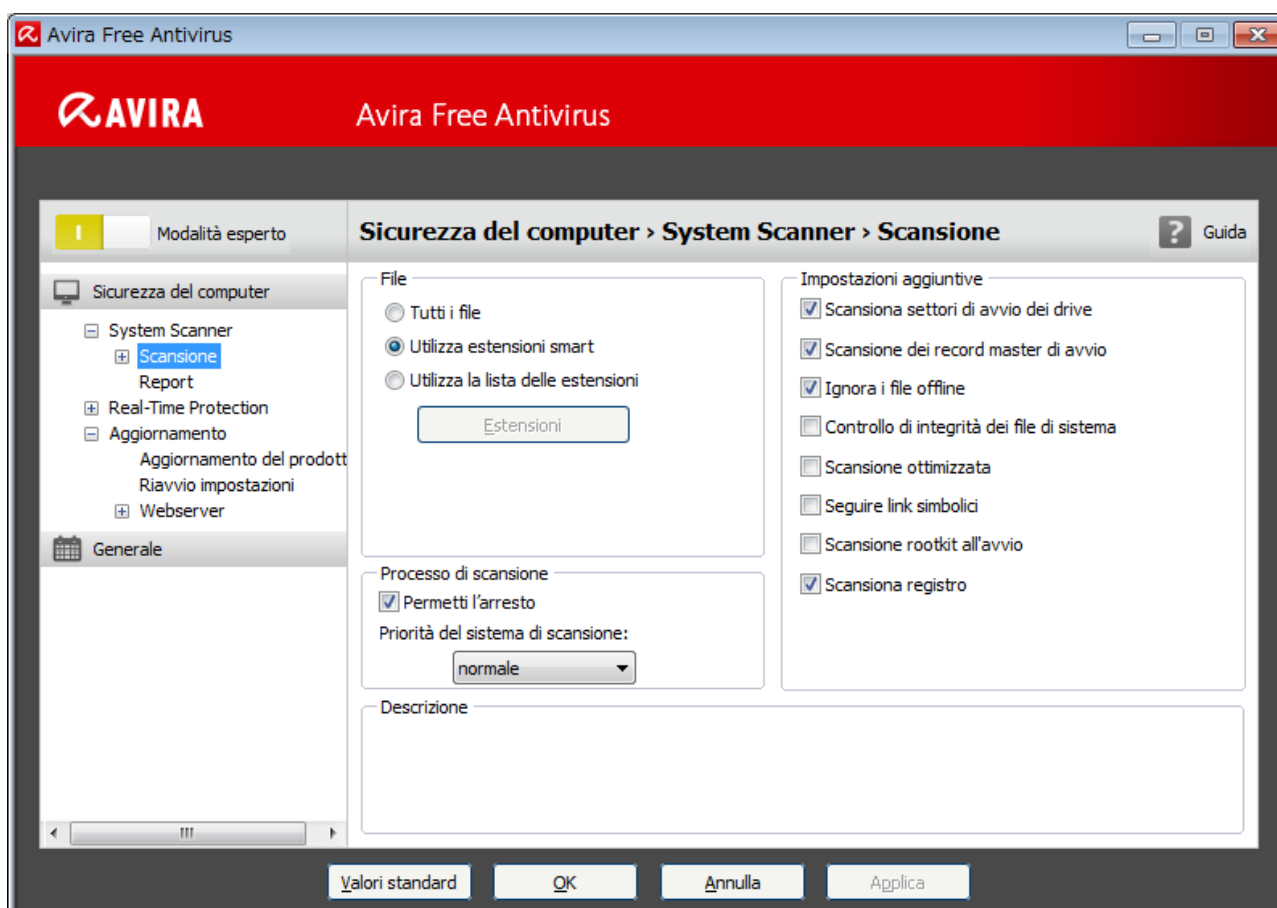
- **Stato**: nella schermata iniziale **Stato** sono presenti tutte le rubriche per controllare le funzionalità del programma (vedere Stato).
  - La finestra **Stato** offre la possibilità di visualizzare quali moduli sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato.
- *SICUREZZA DEL COMPUTER*: in questa rubrica sono disponibili i componenti con cui eseguire la scansione di virus e malware nei file del computer.
  - La rubrica **Scansione** consente di configurare o avviare la scansione diretta in modo semplice (vedere System Scanner). I profili predefiniti consentono di eseguire una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (viene memorizzata), è possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.

- *SICUREZZA INTERNET*: contiene i componenti che consentono di proteggere il computer da virus e malware provenienti da Internet, nonché da accessi di rete indesiderati.

  - La rubrica **Web Protection** visualizza informazioni sugli URL scansionati e sui virus individuati, nonché ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e consente di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.

- *PROTEZIONE DEI BAMBINI*: contiene i tool per consentire ai bambini di navigare su Internet in sicurezza.
- *PROTEZIONE MOBILE*: dalla categoria Avira Free Android Security è possibile accedere online ai dispositivi Android.
  - **Avira Free Android Security** consente di amministrare tutti i dispositivi basati sul sistema operativo Android.
- *AMMINISTRAZIONE*: contiene i tool per l'isolamento e l'amministrazione dei file sospetti o infetti e la pianificazione delle attività ricorrenti.
  - Nella rubrica **Quarantena** è disponibile il cosiddetto Gestore della quarantena, la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena (vedere Quarantena). Inoltre esiste la possibilità di inviare un file selezionato per e-mail all'Avira Malware Research Center.
  - La rubrica **Pianificatore** consente di creare job temporizzati di controllo e di aggiornamento nonché di backup e di cancellare o modificare job esistenti (vedere Pianificatore).
  - La rubrica **Report** consente di visualizzare i risultati delle azioni eseguite (vedere Report).
  - La rubrica **Eventi** consente di ottenere informazioni sugli eventi generati dai moduli del programma (vedere Eventi).

4.1.2 Configurazione

In Configurazione è possibile effettuare le impostazioni per il prodotto Avira in uso. Dopo l'installazione, il prodotto Avira è configurato con le impostazioni standard che assicurano la protezione ottimale del computer. Ciononostante, il computer o le richieste dell'utente per il prodotto Avira possono possedere caratteristiche particolari e richiedere un adattamento delle componenti di protezione del programma.

La Configurazione è strutturata come una finestra di dialogo: con i pulsanti **OK** o **Applica** si memorizzano le impostazioni scelte durante la configurazione, con **Annulla** si rifiutano le impostazioni, con il pulsante **Valori standard** è possibile ripristinare le impostazioni dei valori standard della configurazione. Nella barra di navigazione a sinistra è possibile selezionare singole rubriche di configurazione.

Richiamo della Configurazione

Esistono diverse possibilità per richiamare la configurazione:

- Dal Pannello di controllo di Windows.
- Dal Centro sicurezza PC a partire da Windows XP Service Pack 2.
- Mediante l'icona Tray del programma Avira.
- Nel Control Center mediante la voce di menu Extra > Configurazione.
- Nel Control Center mediante il pulsante Configurazione.

> **Nota**
> Se si richiama la configurazione con il pulsante **Configurazione** in Control Center, si giunge nel registro di configurazione della rubrica attiva in Control Center. Per selezionare un singolo registro di configurazione, è necessario

attivare la **modalità esperto** della configurazione. In questo caso appare una finestra di dialogo, in cui viene richiesto di attivare la **modalità esperto**.

Utilizzo della Configurazione

All'interno della finestra di configurazione si può navigare come in Esplora risorse di Windows:

- Fare clic su una voce della struttura ad albero per visualizzare questa categoria di configurazione nella finestra dei dettagli.
- Fare clic sul segno + prima delle voci per estendere la categoria di configurazione e visualizzare le rubriche di configurazione subordinate nella struttura ad albero.
- Per nascondere le rubriche di configurazione subordinate fare clic sul segno **-** prima della categoria di configurazione estesa.

Nota
Per attivare o disattivare le opzioni nella Configurazione e per premere i pulsanti, è possibile utilizzare le combinazioni di tasti [**Alt**] + carattere sottolineato nel nome dell'opzione o nella definizione del pulsante.

Nota
Le rubriche di configurazione vengono visualizzate per intero nella modalità esperto. Attivare la **modalità esperto** per visualizzare tutte le rubriche di configurazione. La **modalità esperto** può essere protetta con una password da digitare al momento dell'attivazione.

Se si desidera applicare le impostazioni nella configurazione:

- Fare clic sul pulsante **OK**.

  ↳ La finestra di configurazione viene chiusa e le impostazioni applicate.

  - OPPURE -

  Fare clic sul pulsante **Applica**.

  ↳ Le impostazioni vengono applicate. La finestra di configurazione rimane aperta.

Se si desidera terminare la configurazione senza applicare le impostazioni:

- Fare clic sul pulsante **Annulla**.

  ↳ La finestra di configurazione si chiude e le impostazioni vengono ignorate.

Se si desidera ripristinare tutte le impostazioni dei valori standard nella configurazione:

- Fare clic su **Valori standard**.

↳ Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.

Opzioni di configurazione in sintesi

Sono disponibili le seguenti opzioni di configurazione:

- **System Scanner**: configurazione della scansione diretta
  - Opzioni di scansione
  - Azione in caso di rilevamento
  - Opzioni per la scansione degli archivi
  - Eccezioni della scansione diretta
  - Euristica della scansione diretta
  - Impostazione della funzione di report
- **Real-Time Protection**: configurazione della scansione in tempo reale
  - Opzioni di scansione
  - Azione in caso di rilevamento
  - Altre azioni
  - Eccezioni della scansione in tempo reale
  - Euristica della scansione in tempo reale
  - Impostazione della funzione di report
- **Aggiornamento**: configurazione delle impostazioni di aggiornamento
- **Web Protection**: configurazione di Web Protection
  - Opzioni di scansione, attivazione e disattivazione di Web Protection
  - Azione in caso di rilevamento
  - Accessi bloccati: tipi di file e tipi di MIME indesiderati
  - Eccezioni di scansioni di Web Protection: URL, tipi di file, tipi di MIME
  - Euristica di Web Protection
  - Impostazione della funzione di report
- **Generale**:
  - Categorie estese delle minacce per la scansione diretta e in tempo reale
  - Filtro applicazioni: blocco o autorizzazione delle applicazioni
  - Protezione con password per l'accesso al Control Center e alla configurazione
  - Sicurezza: blocco delle funzioni di esecuzione automatica, blocco dei file host di Windows, protezione del prodotto
  - WMI: attiva supporto WMI
  - Configurazione del log eventi
  - Configurazione delle funzioni di report
  - Impostazione delle directory utilizzate
  - Configurazione degli avvisi acustici in caso di rilevamento malware

4.1.3 Icona Tray

Dopo l'installazione, l'icona Tray del prodotto Avira è collocata nella barra delle applicazioni:

Icona	Descrizione
	Avira Real-Time Protection è attivo
	Avira Real-Time Protection non è attivo

L'icona Tray mostra lo stato di Real-Time Protection .

Le funzioni principali del prodotto Avira sono facilmente accessibili mediante il menu contestuale dell'icona Tray.

- Per richiamare il menu contestuale, fare clic con il tasto destro del mouse sull'icona Tray.

Voci del menu contestuale

- **Attiva Real-Time Protection**: attiva o disattiva Avira Real-Time Protection.
- **Attiva Web Protection**: attiva o disattiva Avira Web Protection.
- **Avvia Avira Free Antivirus**: apre Control Center.
- **Configura Avira Free Antivirus** : apre la configurazione.
- **I miei messaggi**: apre una finestra con i messaggi più recenti relativi al prodotto Avira.
- **Avvia l'aggiornamento**: avvia un aggiornamento.
- **Guida in linea**: apre la guida in linea.
- **Informazioni su Avira Free Antivirus:** apre una finestra di dialogo con informazioni sul prodotto Avira: prodotto, versione e licenza.
- **Avira su Internet**: apre il portale Web di Avira su Internet. Il prerequisito essenziale è l'accesso attivo a Internet.

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar contiene due componenti principali: Avira SearchFree e la Toolbar già nota.

La nuova Avira SearchFree Toolbar viene installata come componente aggiuntivo. Quando si richiama per la prima volta il browser (con Internet Explorer e Firefox) verrà chiesto se si consente la modifica del browser dell'utente da parte del programma Avira

SearchFree Toolbar. Per terminare con successo l'installazione di Avira SearchFree Toolbar, l'utente dovrà accettare.

Avira SearchFree è il nuovo motore di ricerca di Avira e contiene un logo Avira, su cui si può fare clic, che conduce alla pagina web di Avira e anche in canali web e video. Consente agli utenti di Avira di effettuare una ricerca ampia e sicura.

La Toolbar è integrata nel browser Web ed è formata da un campo di ricerca, un logo Avira collegato alla pagina web di Avira, due display di stato, tre widget e il menu **Opzioni**.

- Barra di ricerca
  Utilizzare la barra di ricerca per effettuare ricerche in Internet in modo veloce e gratuito tramite il motore di ricerca Avira SearchFree.
- Display di stato
  I display di stato indicano lo stato di Web Protection e l'attuale stato di aggiornamento del prodotto Avira, aiutando l'utente a riconoscere quali azioni devono essere eseguite per proteggere il PC.
- Widget
  Avira fornisce un accesso diretto alle funzioni più importanti su Internet, ad esempio alle notizie dell'utente su Facebook o alla sua casella e-mail. È anche possibile determinare la sicurezza del sistema dell'utente attraverso il widget sicurezza del browser (solo per Firefox e Internet Explorer).
- Opzioni
  Tramite il menu Opzioni è possibile accedere alle Opzioni della toolbar, cancellare la cronologia delle ricerche, richiamare la Guida in linea e le Informazioni relative alla toolbar e disinstallare l'Avira SearchFree Toolbar direttamente tramite browser Web (solo per Firefox e Internet Explorer).

4.2.1 Utilizzo

Barra di ricerca

Tramite la barra di ricerca è possibile ricercare su Internet uno o più termini.

Per fare questo inserire il termine desiderato nel campo di ricerca e premere poi il pulsante **Invio** o fare clic su **Cerca**. Il motore di ricerca Avira SearchFree esegue la ricerca su Internet e mostra poi tutti i risultati riscontrati nella finestra del browser.

La procedura per eseguire la configurazione personalizzata di Avira SearchFree in Internet Explorer, Firefox e Chrome è contenuta in **Opzioni.**

Display di stato

Web Protection

Sulla sinistra si trova l'avviso di stato, che fornisce informazioni su Web Protection di Avira.

Icona	Display di stato	Descrizione
	Web Protection	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira Web Protection è attivo. Il computer è protetto.* Ciò significa che non sono necessarie ulteriori azioni.
	Web Protection	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira Web Protection è disattivato. Controllare il software Avira per attivare Web Protection.*
	Sin Web Protection	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Nessun antivirus Avira installato. Il computer potrebbe essere in pericolo.* Ciò potrebbe significare che il prodotto Avira in uso è disinstallato oppure che non è stato installato correttamente. ↪ Si viene così rimandati al sito Web di Avira, da cui è possibile scaricare il prodotto Avira.
	Non disponibile	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira non è disponibile. Per essere sicuri che la protezione del PC è ancora attiva, controllare se il software di Avira è ancora installato sul computer e se è eseguito.* ▶ Fare clic sul simbolo grigio o sul testo per collegarsi alla pagina di aiuto di Avira. Qui verranno fornite ulteriori informazioni su come procedere.
	Errore	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira ha comunicato un errore.* ▶ Fare clic sul simbolo grigio o sul testo per collegarsi alla pagina di supporto di Avira.

Widget

Avira SearchFree Toolbar dispone di 3 widget con le più importanti funzioni di Internet: Facebook, e-mail e Web Protection.

Facebook

Questa funzione consente di ricevere direttamente le comunicazioni di Facebook e quindi di rimanere sempre aggiornato.

E-mail

Quando si fa clic sul simbolo e-mail viene visualizzato un elenco a discesa in cui è possibile scegliere tra i provider più utilizzati.

Web Protection

Questo widget è stato sviluppato da Avira per raggiungere in modo particolarmente semplice tutte le opzioni di sicurezza di Internet. Al momento è disponibile soltanto per Firefox e Internet Explorer. Sono offerte differenti opzioni che si possono chiamare in modo differente a seconda del browser:

- *Blocco pop-up*

Se questa opzione è attiva quando si naviga su Internet verranno bloccate tutte le finestre pop-up.

- *Blocco cookie*

Se questa opzione è attiva non verrà salvato alcun cookie durante l'utilizzo del browser.

- *Navigazione anonima (Firefox) / In Private Browsen (Internet Explorer)*

Se questa opzione è attiva, quando si naviga su Internet non si lasciano tracce. Quest'opzione non è disponibile per Internet Explorer 7 e 8.

- *Cancella cronologia recente (Firefox) / Cancellazione della cronologia di navigazione (Internet Explorer)*

Con questa opzione si cancellano tutte le precedenti attività di Internet.

Website Safety Advisor

Website Safety Advisor offre una classificazione della sicurezza durante la navigazione su Internet.
In questo modo è possibile valutare se la pagina Web che si sta visitando rappresenta un rischio per la sicurezza.
Questo widget offre inoltre altre informazioni sul sito Web, ad esempio il proprietario del dominio o il motivo per cui il sito Web è stato inserito in una determinata categoria.
I livelli di sicurezza sono tre: sicuro, poco rischioso e molto rischioso.

I livelli di sicurezza vengono indicati nella toolbar e nei risultati della ricerca, sotto forma dell'icona Avira Tray, con i seguenti simboli:

Icona	Display di stato	Descrizione
	Sicuro	I siti Web sono contrassegnati da un segno di spunta verde.
	Poco rischioso	I siti Web moderatamente rischiosi sono contrassegnati da un punto esclamativo giallo.
	Molto rischioso	I siti Web molto rischiosi sono contrassegnati dal segnale rosso di stop.
	Fallito	Un punto di domanda grigio indica i siti Web il cui rischio non può essere valutato.
	Controllo in corso	Questo segno compare durante la verifica dello stato.

Browser Tracking Blocker

Browser Tracking Blocker permette di interrompere le procedure di raccolta dei dati dell'utente mentre si naviga su Internet.
Il widget consente di selezionare quali rilevamenti bloccare e quali consentire.

Le aziende si dividono in tre categorie:

- Social network
- Ad network
- Altre aziende

4.2.2 Opzioni

Avira SearchFree Toolbar è compatibile con Internet Explorer, Firefox e Google Chrome e può essere configurata in entrambi i browser Web in base alle esigenze dell'utente:

- Opzioni di configurazione con Internet Explorer
- Opzioni di configurazione con Firefox
- Opzioni di configurazione con Chrome

Internet Explorer

Nel browser Web Internet Explorer, nel menu **Opzioni**, sono disponibili le seguenti opzioni di configurazione per l'Avira SearchFree Toolbar:

Opzioni della Toolbar

Scansione

Seleziona motore Avira

Nel menu **Seleziona motore Avira** è possibile selezionare quale motore di ricerca deve essere utilizzato per la ricerca. Sono disponibili motori di ricerca delle seguenti zone: USA, Brasile, Germania, Spagna, Europa, Francia, Italia, Paesi Bassi, Russia e Gran Bretagna.

Avvia ricerche in

Nel menu dell'opzione **Avvia ricerche in** è possibile selezionare dove deve essere visualizzato il risultato di una ricerca, se nella **Finestra attiva**, in una **nuova finestra** oppure su una**nuova scheda**.

Mostra ultime ricerche

Se l'opzione **Mostra ultime ricerche** è attiva, sotto al campo di inserimento testo della barra di ricerca vengono visualizzati i termini di ricerca digitati fino a quel momento.

Azzera la cronologia delle ricerche all'uscita del browser

Attivare l'opzione **Azzera la cronologia delle ricerche all'uscita del browser** quando non si vuole salvare la cronologia delle ricerche già effettuate e si desidera che venga cancellata alla chiusura del browser Web.

Altre opzioni

Seleziona lingua barra

In **Seleziona lingua barra** è possibile selezionare la lingua di Avira SearchFree Toolbar. Sono disponibili le versioni in inglese, tedesco, spagnolo, francese, italiano, portoghese e olandese.

> **Nota**
> La lingua preimpostata dell'Avira SearchFree Toolbar corrisponde a quella del programma dell'utente, se disponibile. Se la toolbar non è disponibile nella lingua dell'utente, viene preimpostata la lingua inglese.

Visualizza i nomi dei pulsanti

Disattivare l'opzione **Visualizza i nomi dei pulsanti** se si desidera nascondere il testo accanto alle icone di Avira SearchFree Toolbar.

Azzera cronologia delle ricerche

Attivare l'opzione **Azzera cronologia delle ricerche** se non si desidera salvare le ricerche già eseguite, bensì cancellarle subito.

Guida in linea

Fare clic su **Guida in linea** per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Disinstalla

È possibile disinstallare l'Avira SearchFree Toolbar anche direttamente in Internet Explorer: Disinstallazione mediante il browser Web.

Info

Fare clic su **Info** per sapere quale versione di Avira SearchFree Toolbar è installata.

Firefox

Nel browser Web Firefox, nel menu **Opzioni**, sono disponibili le seguenti opzioni di configurazione per l'Avira SearchFree Toolbar:

Opzioni della Toolbar

Scansione

Seleziona motore Avira

Nel menu **Seleziona motore Avira** è possibile selezionare quale motore di ricerca deve essere utilizzato per la ricerca. Sono disponibili motori di ricerca delle seguenti zone: USA, Brasile, Germania, Spagna, Europa, Francia, Italia, Paesi Bassi, Russia e Gran Bretagna.

Mostra ultime ricerche

Se l'opzione **Mostra ultime ricerche** è attiva, è possibile visualizzare i termini di ricerca digitati fino a quel momento, facendo clic sulla freccia nella barra di ricerca. Selezionare uno dei termini se si vuole visualizzare nuovamente il risultato di tale ricerca.

Azzera la cronologia delle ricerche all'uscita del browser

Attivare l'opzione **Azzera la cronologia delle ricerche all'uscita del browser** quando non si vuole salvare la cronologia delle ricerche già effettuate e si desidera che venga cancellata alla chiusura del browser Web.

Mostra i risultati della ricerca di Ask, quando vengono inseriti indirizzi URL non validi o parole chiave nel campo degli indirizzi del browser

Se questa opzione è attiva, ogni volta che parole chiave o indirizzi URL non validi vengono inseriti nel campo degli indirizzi del browser, viene avviata una ricerca e mostrati i relativi risultati.

Altre opzioni

Seleziona lingua barra

In **Seleziona lingua barra** è possibile selezionare la lingua di Avira SearchFree Toolbar. Sono disponibili le versioni in inglese, tedesco, spagnolo, francese, italiano, portoghese e olandese.

> **Nota**
> La lingua preimpostata dell'Avira SearchFree Toolbar corrisponde a quella del programma dell'utente, se disponibile. Se la toolbar non è disponibile nella lingua dell'utente, viene preimpostata la lingua inglese.

Visualizza i nomi dei pulsanti

Disattivare l'opzione **Visualizza i nomi dei pulsanti** se si desidera nascondere il testo accanto alle icone di Avira SearchFree Toolbar.

Azzera cronologia delle ricerche

Attivare l'opzione **Azzera cronologia delle ricerche** se non si desidera salvare le ricerche già eseguite, bensì cancellarle subito.

Guida in linea

Fare clic su **Guida in linea** per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Disinstalla

È possibile disinstallare l'Avira SearchFree Toolbar anche direttamente in Internet Explorer: Disinstallazione mediante il browser Web.

Info

Fare clic su **Info** per sapere quale versione di Avira SearchFree Toolbar è installata.

Chrome

Nel browser Web Google Chrome tutte le opzioni di configurazione sono sotto l'ombrello rosso di Avira. Per l'Avira SearchFree Toolbar sono disponibili le seguenti opzioni:

Guida in linea

Fare clic su **Guida in linea** per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Istruzioni per la disinstallazione

Qui è possibile trovare i collegamenti alle istruzioni sulla disinstallazione di Avira SearchFree Toolbar.

Info

Fare clic su **Info** per sapere quale versione di Avira SearchFree Toolbar è installata.

Mostra e nascondi Avira SearchFree Toolbar

Questa voce del menù attiva e disattiva Avira SearchFree, che si trova nella parte alta della finestra.

4.2.3 Disinstallazione

Si può disinstallare Avira SearchFree Toolbar (descritto ad esempio per Windows 7) nel seguente modo:

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.
- Fare doppio clic su **Programmi e funzionalità**.
- Selezionare **Avira SearchFree Toolbar plus Web Protection** nell'elenco e fare clic su **Disinstalla**.
  - ↳ Verrà chiesto all'utente se desidera davvero disinstallare il prodotto.
- Confermare con **Sì**.
  - ↳ Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

Disinstallazione mediante il browser Web

È inoltre possibile disinstallare l'Avira SearchFree Toolbar in **Firefox e Internet Explorer** direttamente dal browser:

- Aprire nella barra di ricerca a destra il menu **Opzioni**.
- Fare clic su **Disinstalla**.
  - ↳ Viene richiesto di chiudere il browser Web, se ancora aperto.
- Chiudere il browser Web e fare clic su **OK**.
  - ↳ Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

> **Nota**
> Quando si disinstalla Avira SearchFree Toolbar, viene disinstallato anche Web Protection.

> **Nota**
> Per disinstallare Avira SearchFree Toolbar, il toolbar deve essere attivato in Add-On Manager.

Disinstallazione come Add-On

Poiché l'ultima versione di Avira SearchFree è installata come Add-On, è anche possibile gestire il tool con differenti manager di Add-On.

Firefox

Fare clic su **Strumenti > Add-ons > Estensioni**. Qui è possibile gestire l'Add-on di Avira, ossia attivare e disattivare o disinstallare.

Internet Explorer

Fare clic su **Gestione Add-ons > Barra degli strumenti ed Estensioni**. Qui è possibile attivare e disattivare o disinstallare l'Add-on di Avira.

Google Chrome

L'Add-on di Avira può essere gestito facendo clic su **Opzioni > Estensioni**. Ciò consente di attivare, disattivare o disinstallare la toolbar.

4.3 Come procedere

Nei capitoli "Come procedere" viene fornita una breve panoramica dell'attivazione della licenza e del prodotto e delle funzioni principali del prodotto Avira in uso. I brevi passaggi selezionati permettono di farsi un'idea delle funzionalità del prodotto Avira. Tali passaggi non sostituiscono tuttavia le spiegazioni complete nei singoli capitoli della guida.

4.3.1 Esecuzione degli aggiornamenti automatici

Per creare con Avira Pianificatore un job con cui aggiornare automaticamente il prodotto Avira in uso:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Pianificatore** in Control Center.
- Fare clic sull'icona [+] **Inserisci nuovo job**.
  - ↳ Verrà visualizzata la finestra di dialogo **Nome e descrizione del job**.

- Assegnare un nome al job ed eventualmente descriverlo.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Tipo di job**.
- Selezionare un **Job di aggiornamento** dalla lista.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguito l'aggiornamento:

- **Immediatamente**
- **Ogni giorno**
- **Ogni settimana**
- **Intervallo**
- **Singolo**

> **Nota**
> Si consiglia di eseguire regolarmente e spesso aggiornamenti automatici. L'intervallo di aggiornamento consigliato è: 6 Ore.

- Indicare il termine in base alla selezione.
- Eventualmente selezionare anche le seguenti opzioni aggiuntive (disponibili in base al tipo di job):

- **Ripeti il job a tempo già scaduto**
  Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Selezione della modalità di visualizzazione**.
- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotto**: solo la barra di avanzamento
- **Espanso**: tutta la finestra del job

- Fare clic su **Fine**.
  - ↳ Il nuovo job assegnato viene visualizzato nello schermo home della rubrica *AMMINISTRAZIONE* **> Pianificatore** come attivato (segno di spunta).
- Disattivare i job che non devono essere eseguiti.

Mediante le seguenti icone, è possibile elaborare ulteriormente i job:

i Visualizzazione delle proprietà di un job

Modifica del job

Eliminazione del job

Avvio del job

Interruzione del job

4.3.2 Avvio di un aggiornamento manuale

Esistono vari modi di avviare manualmente un aggiornamento: durante gli aggiornamenti avviati manualmente viene sempre eseguito anche l'aggiornamento del file di definizione dei virus e del motore di ricerca.

Per avviare manualmente un aggiornamento del prodotto Avira:

- Fare clic con il tasto destro del mouse sull'icona Tray di Avira nella barra delle applicazioni e selezionare **Avvia aggiornamento**.

  \- OPPURE -

- In Control Center selezionare la rubrica **Stato**, quindi fare clic sul link **Avvia aggiornamento** nel riquadro **Ultimo aggiornamento**.

  \- OPPURE -

  In Control Center, nel menu **Aggiornamento**, selezionare il comando **Avvia aggiornamento**.

  ↳ Verrà visualizzata la finestra di dialogo **Updater**.

Nota
Si consiglia di eseguire regolarmente aggiornamenti automatici. L'intervallo di aggiornamento consigliato è: 6 Ore.

Nota
È possibile eseguire un aggiornamento anche manualmente mediante il Centro di sicurezza PC di Windows.

4.3.3 Scansione diretta: scansione di virus e malware con un profilo di scansione

Un profilo di scansione è un insieme di drive e directory che devono essere scansionati.

Per effettuare una scansione con un profilo di scansione è possibile:

- Utilizzare il profilo di scansione predefinito

  Se i profili di scansione predefiniti rispondono alle esigenze dell'utente.
- Modificare il profilo di scansione e utilizzarlo (selezione manuale)

  Se si desidera eseguire una scansione con un profilo di scansione personalizzato.

In base al sistema operativo sono disponibili diverse icone per l'avvio di un profilo di scansione:

- In Windows XP:

  Con quest'icona si avvia la scansione mediante un profilo di scansione.
- In Windows Vista:

  In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati, ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

  Selezionando quest'icona si avvia una scansione limitata mediante un profilo di scansione. Vengono scansionati solo i file e le directory per cui Windows Vista ha concesso i diritti di accesso.

  Con quest'icona si avvia una scansione con diritti avanzati dell'amministratore. Dopo una conferma, vengono scansionati tutti i file e le directory del profilo di scansione selezionato.

Per cercare virus e malware con un profilo di scansione:

- Selezionare la rubrica *PROTEZIONE PC* **> System Scanner** in Control Center.
  - ↳ Verranno visualizzati i profili di scansione predefiniti.
- Selezionare uno dei profili di scansione predefiniti.

  \- OPPURE -

  Modificare il profilo di scansione in **Selezione manuale**.
- Fare clic sull'icona (Windows XP: oppure Windows Vista:).
- Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

Se si desidera modificare un profilo di scansione:

- Aprire nel profilo di ricerca **Selezione manuale** la struttura dei file fin quando non vengono aperti tutti i drive che devono essere scansionati:
- Selezionare i nodi che devono essere scansionati facendo clic nella casella:

4.3.4 Scansione diretta: ricerca di virus e malware con Drag&Drop

È possibile cercare con Drag&Drop virus e malware come segue:

✓ Il Control Center del programma Avira è aperto.

- Selezionare il file, che si desidera scansionare.
- Trascinare con il tasto sinistro del mouse il file selezionato in Control Center.
  - ↳ Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.5 Scansione diretta: Scansione di virus e malware con il menu contestuale

Per eseguire una scansione mirata in cerca di virus e malware mediante il menu contestuale:

- Fare clic (ad esempio in Esplora risorse di Windows, sul desktop o in una directory aperta di Windows) con il pulsante destro del mouse sul file chesi desidera controllare.
  - ↳ Verrà visualizzato il menu contestuale di Esplora risorse di Windows.
- Nel menu contestuale selezionare **Controlla i file selezionati con Avira**.
  - ↳ Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.6 Scansione diretta: ricerca automatica di virus e malware

> **Nota**
> Dopo l'installazione, il job di scansione *Scansione completa del sistema* viene creato nel pianificatore: la scansione completa del sistema viene eseguita automaticamente alla frequenza consigliata.

Come creare un job di scansione automatica di virus e malware:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Pianificatore** in Control Center.
- Fare clic sull'icona [+] **Inserisci un nuovo job**.
  - ↳ Verrà visualizzata la finestra di dialogo **Nome e descrizione del job**.
- Assegnare un nome al job ed eventualmente descriverlo.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Tipo di job**.
- Selezionare il **Job di scansione**.
- Fare clic su **Avanti**.

↳ Verrà visualizzata la finestra di dialogo **Selezione del profilo**.

- Selezionare quale profilo deve essere scansionato.
- Fare clic su **Avanti**.

↳ Verrà visualizzata la finestra di dialogo **Durata del job**.

- Selezionare quando deve essere eseguita la scansione:

- **Immediatamente**
- **Ogni giorno**
- **Ogni settimana**
- **Intervallo**
- **Singolo**

- Indicare il termine in base alla selezione.
- Eventualmente selezionare la seguente opzione supplementare (disponibile in base al tipo di job): **Ripeti il job a tempo già scaduto**

↳ Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

- Fare clic su **Avanti**.

↳ Verrà visualizzata la finestra di dialogo **Selezione della modalità di visualizzazione**.

- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotto**: solo la barra di avanzamento
- **Espanso**: tutta la finestra del job

- Selezionare l'opzione **Spegni computer al termine del job** se si desidera che il computer si spenga automaticamente non appena il job è stato eseguito e concluso.

L'opzione è disponibile solo nella modalità di visualizzazione ridotta o estesa.

- Fare clic su **Fine**.

↳ Il nuovo job creato viene visualizzato nella schermata iniziale della rubrica *AMMINISTRAZIONE* **> Pianificatore** come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante le seguenti icone, è possibile elaborare ulteriormente i job:

i Visualizzazione delle proprietà di un job

Modifica del job

Eliminazione del job

▶ Avvio del job

■ Interruzione del job

4.3.7 Scansione diretta: scansione mirata in cerca di rootkit attivi

Per effettuare una scansione in cerca di rootkit attivi utilizzare il profilo di scansione predefinito **Scansione alla ricerca di rootkit e malware attivi**.

La ricerca di rootkit mirata si effettua nel modo seguente:

- Selezionare la rubrica *PROTEZIONE PC* **> System Scanner** in Control Center.
  ↳ Verranno visualizzati i profili di ricerca predefiniti.
- Selezionare il profilo di ricerca predefinito **Scansione alla ricerca di rootkit e malware attivi**.
- Evidenziare altri eventuali nodi e directory da verificare con un clic nella casella del livello della directory.
- Fare clic sull'icona (Windows XP: oppure Windows Vista:).
  ↳ Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.
  ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.8 Reazione a virus e malware riscontrati

Per i singoli componenti di protezione del prodotto Avira è possibile impostare nella configurazione, nella rubrica **Azione in caso di rilevamento**, la reazione desiderata del prodotto Avira in caso di rilevamento di un virus o di un programma indesiderato.

Nel componente Real-Time Protection non esiste la possibilità di configurare alcuna opzione di azione. In caso di rilevamento di un virus compare un messaggio sul desktop. È possibile rimuovere il malware rilevato direttamente nel messaggio sul desktop, oppure trasmettere il malware al componente System Scanner per un ulteriore trattamento del virus selezionando il pulsante **Dettagli**. System Scanner notifica il rilevamento tramite una finestra con un menu contestuale contenente diverse opzioni per trattare il file infetto (vedere Rilevamento > System Scanner).

Opzioni di azione in System Scanner:

- **Interattivo**

  Nella modalità di azione interattiva vengono comunicati i rilevamenti della scansione di System Scanner in una finestra di dialogo. Quest'impostazione è attivata di default.
  Al termine della **scansione di System Scanner**, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da

eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure chiudere System Scanner.

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Web Protection:

- **Interattivo**

  Nella modalità di azione interattiva, in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come gestire i file infetti. Quest'impostazione è attivata di default.

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Modalità di azione interattiva

- Nella modalità di azione interattiva si reagisce ai virus e ai programmi indesiderati rilevati selezionando nell'avviso un'**azione per gli oggetti infetti** ed eseguendo l'azione selezionata mediante **Conferma**.

Per il trattamento di oggetti infetti possono essere selezionate le seguenti azioni:

> **Nota**
> Le azioni disponibili dipendono dal sistema operativo, dal componente di protezione (Avira System Scanner, Avira Real-Time Protection, Avira Web Protection), che segnala il file rilevato, e dal malware rilevato.

Azioni di System Scanner:

- **Ripara**

  Il file viene riparato.
  Questa opzione è attivabile solo se è possibile riparare il file.

- **Rinomina**

  Il file viene rinominato in **.vir*. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

- **Quarantena**

  Il file viene compresso in un formato speciale (**.qua*) e spostato nella directory di quarantena *INFECTED* sull'hard disk, in modo da escludere qualsiasi accesso

diretto. I file in questa directory possono essere successivamente riparati nella quarantena o, se necessario, inviati ad Avira.

- **Elimina**

  Il file viene eliminato.
  Se il file rilevato è un virus del record di avvio, eliminandolo viene cancellato il record di avvio. Viene scritto un nuovo record di avvio.

- **Ignora**

  Non vengono eseguite ulteriori azioni. Il file infetto rimane attivo sul computer.

> **Avviso**
> Pericolo di perdita di dati e danni al sistema operativo del computer!
> Utilizzare l'opzione **Ignora** solo in casi eccezionali e fondati.

- **Ignora sempre**

  Opzione di azione in caso di rilevamento di Real-Time Protection: Real-Time Protection non esegue nessun'altra azione. L'accesso al file è consentito. Tutti gli ulteriori accessi a questo file sono consentiti e non vengono più segnalati fino al riavvio del computer o all'aggiornamento del file di definizione dei virus.

- **Copia in quarantena**

  Opzione di azione in caso di rilevamento di un rootkit: il rilevamento viene copiato in quarantena.

- **Ripara record di avvio | Scarica strumento di riparazione**

  Opzioni di azione in caso di rilevamento di record di avvio: sono disponibili opzioni per la riparazione per le unità floppy infette. Se con il prodotto Avira non è possibile effettuare alcuna riparazione, è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

> **Nota**
> Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

Azioni di Web Protection:

- **Nega accesso**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso.

- **Quarantena**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono spostati nella quarantena. Il file infetto può essere ripristinato dal Gestore della quarantena se ha

un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

- **Ignora**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web.

> **Avviso**
> In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali e fondati.

> **Nota**
> Consigliamo di spostare in quarantena un file sospetto che non può essere riparato.

4.3.9 Quarantena: trattamento dei file (*.qua) in quarantena

È possibile trattare i file in quarantena nel modo seguente:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Quarantena** in Control Center.
- Verificare di quali file si tratta cosicché sia possibile ripristinare gli originali sul computer.

Se si desidera visualizzare maggiori informazioni su un file:

- Selezionare il file e fare clic su [i] .
  - ↳ Verrà visualizzata la finestra di dialogo **Proprietà** con ulteriori informazioni sul file.

Se si desidera scansionare nuovamente un file:

La scansione di un file è consigliata quando il file di definizione dei virus del prodotto Avira è stato aggiornato ed esiste il sospetto di un falso allarme. È così possibile confermare un falso allarme a una successiva verifica e ripristinare il file.

- Selezionare il file e fare clic su [🔍] .
  - ↳ Il file viene controllato utilizzando le impostazioni della scansione diretta per virus e malware.
  - ↳ Dopo il controllo appare la finestra di dialogo **Statistiche della scansione** in cui viene visualizzata la statistica relativa allo stato del file prima e dopo la nuova scansione.

Se si desidera eliminare un file:

- Selezionare il file e fare clic su .
- Confermare la selezione con **Sì**.

Se si desidera caricare il file da analizzare su un server Web di Avira Malware Research Center:

- Selezionare il file che si desidera caricare.
- Fare clic su .
  - ↳ Si aprirà la finestra di dialogo *Upload file* con un modulo per inserire i dati personali a cui essere contattati.
- Indicare per intero i propri dati.
- Scegliere un tipo:: **File sospetto** o **Sospetto di falso positivo**.
- Selezionare un formato di risposta: **HTML**, **Testo**, **HTML & Testo**.
- Fare clic su **OK.**
  - ↳ Il file compresso viene caricato su un server Web di Avira Malware Research Center.

> **Nota**
> Nei seguenti casi si consiglia di eseguire un'analisi con Avira Malware Research Center:
> **Riscontro euristico (file sospetto)**: Durante una scansione un file è stato classificato come sospetto dal prodotto Avira in uso e messo in quarantena: nella finestra di dialogo sul rilevamento del virus oppure nel file di report della scansione viene consigliato di analizzare il file con Avira Malware Research Center.

> **Nota**
> La dimensione dei file caricati si limita a 20 MB non compressi o a 8 MB compressi.

> **Nota**
> È possibile caricare solo un singolo file per volta.

Se si desidera esportare in un file di testo le proprietà di un oggetto in quarantena selezionato:

- Selezionare l'oggetto in quarantena e fare clic su .
  - ↳ Si apre un file di testo con i dati dell'oggetto in quarantena scelto.

- Salvare il file di testo.

I file in quarantena possono essere ripristinati (vedere capitolo: Quarantena: ripristino dei file in quarantena).

4.3.10 Quarantena: ripristino dei file in quarantena

In base al sistema operativo sono disponibili diverse icone per il ripristino:

- **In Windows XP e 2000**:

  Quest'icona consente di ripristinare i file nella directory originale.

  Quest'icona consente di ripristinare i file nella directory selezionata.

- **In Windows Vista**:

  In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati, ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

  Quest'icona consente di ripristinare i file nella directory selezionata.

  Quest'icona consente di ripristinare i file nella directory originale. Se per l'accesso a questa directory sono necessari diritti di amministratore avanzati, appare una richiesta corrispondente.

È possibile ripristinare i file in quarantena nel modo seguente:

Avviso
Pericolo di perdita di dati e danni al sistema operativo del computer! Utilizzare la funzione **Ripristina l'oggetto selezionato** solo in casi eccezionali. Ripristinare solo quei file che possono essere riparati con una nuova scansione.

✓ File nuovamente scansionato e riparato con una scansione.

- Selezionare la rubrica *AMMINISTRAZIONE* **> Quarantena** in Control Center.

Nota
Le e-mail e i relativi allegati possono essere ripristinati soltanto con l'opzione e con l'estensione **.eml*.

Se si desidera ripristinare un file nella sua posizione originale:

- Evidenziare il file e fare clic sull'icona (Windows XP: , Windows Vista).

  Questa opzione non è disponibile per le e-mail.

> **Nota**
> Le e-mail e i relativi allegati possono essere ripristinati soltanto con l'opzione e con l'estensione **.eml*.

↳ Viene richiesto quindi se si desidera ripristinare il file.

- Fare clic su **Sì**.

  ↳ Il file viene ripristinato nella directory dalla quale è stato spostato in quarantena.

Se si desidera ripristinare un file in una determinata directory:

- Selezionare il file e fare clic su .

  ↳ Viene richiesto quindi se si desidera ripristinare il file.
- Fare clic su **Sì**.

  ↳ Verrà visualizzata la finestra standard di Windows per la selezione di una directory.
- Selezionare la directory nella quale si desidera ripristinare il file e confermare.

  ↳ Il file viene ripristinato nella directory selezionata.

4.3.11 Quarantena: spostamento dei file sospetti in quarantena

È possibile spostare in quarantena i file sospetti manualmente come segue:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Quarantena** in Control Center.
- Fare clic su .

  ↳ Apparirà la finestra standard di Windows per la selezione di un file.
- Selezionare il file e confermare facendo clic su **Apri**.

  ↳ Il file viene spostato in quarantena.

I file in quarantena possono essere scansionati con Avira System Scanner (vedere capitolo: Quarantena: trattamento dei file (*.qua) in quarantena).

4.3.12 Profilo di ricerca: Inserire o eliminare un tipo di file in un profilo di ricerca

Per stabilire per un profilo di ricerca i tipi di file da scansionare o i tipi di file che devono essere esclusi dalla ricerca (possibile solo con selezione manuale):

✓ Da Control Center, selezionare la rubrica *SICUREZZA DEL COMPUTER* **> Scansione**.

- Fare clic con il tasto destro del mouse sul profilo di ricerca che si desidera modificare.

↳ Verrà visualizzato un menu contestuale.

- Selezionare la voce **Filtro file**.
- Aprire nuovamente il menu contestuale facendo clic sul piccolo triangolo sul lato destro del menu contestuale.

  ↳ Verranno visualizzate le voci **Standard**, **Scansiona tutti i file** e **Personalizzato**.
- Selezionare la voce **Personalizzato**.

  ↳ Verrà visualizzata la finestra di dialogo **Estensioni file** con un elenco di tutti i tipi di file che devono essere abbinati al profilo di ricerca.

Se si desidera escludere un tipo di file dalla scansione:

- Selezionare il tipo di file e fare clic su **Elimina**.

Se si desidera aggiungere un tipo di file dalla scansione:

- Selezionare un tipo di file.
- Fare clic su **Aggiungi** e inserire l'estensione del tipo di file nel campo.

  Utilizzare un massimo di 10 caratteri e non inserire punti. I caratteri jolly * e ? sono ammessi.

4.3.13 Profilo di ricerca: creazione di un collegamento sul desktop per il profilo di scansione

Mediante un collegamento sul desktop a un profilo di scansione è possibile avviare una scansione diretta facendo clic sul desktop senza richiamare il Control Center del prodotto Avira in uso.

Per creare un collegamento al profilo di scansione dal desktop:

✓ Da Control Center, selezionare la rubrica *SICUREZZA DEL COMPUTER* **> Scansione**.

- Selezionare il profilo di scansione di cui si intende creare il collegamento.
- Fare clic sull'icona .

  ↳ Viene creato un collegamento sul desktop.

4.3.14 Eventi: filtrare eventi

In Control Center, nel menu *AMMINISTRAZIONE* **> Eventi**, vengono visualizzati tutti gli eventi creati dai componenti del programma del prodotto Avira (analogamente alla visualizzazione eventi del sistema operativo Windows). I componenti del programma, in ordine alfabetico, sono i seguenti:

- Web Protection
- Real-Time Protection

- Servizio di assistenza
- Pianificatore
- System Scanner
- Updater

Vengono visualizzati i seguenti tipi di eventi:

- *Informazione*
- *Avviso*
- *Errore*
- *Rilevamento*

Come filtrare gli eventi visualizzati:

- In Control Center selezionare la rubrica *AMMINISTRAZIONE* **> Eventi**.
- Attivare la casella di controllo dei componenti di programma per visualizzare gli eventi dei componenti attivi.

  \- OPPURE -

  Disattivare la casella di controllo dei componenti di programma per non visualizzare gli eventi dei componenti disattivati.
- Attivare la casella di controllo dei tipi di evento per visualizzare questi eventi.

  \- OPPURE -

  Disattivare la casella di controllo dei tipi di evento per non visualizzare questi eventi.

5. System Scanner

Con il componente System Scanner è possibile effettuare scansioni mirate per virus e programmi indesiderati (scansione diretta). È possibile effettuare una scansione per file infetti in diversi modi:

- **Scansione diretta mediante il menu contestuale**
  La scansione diretta mediante il menu contestuale (tasto destro del mouse - voce **Controlla i file selezionati con Avira**) si consiglia quando, ad esempio, si desidera controllare singoli file e directory in Esplora risorse di Windows. Un ulteriore vantaggio è che Control Center non deve essere avviato per la scansione diretta mediante il menu contestuale.
- **Scansione diretta mediante Drag&Drop**
  Trascinando un file o una directory nella finestra di programma del Control Center, System Scanner verifica il file o la directory, nonché tutte le sottodirectory. Questa procedura è consigliata quando si desidera controllare i singoli file e directory che sono stati archiviati, ad esempio, sul desktop.
- **Scansione diretta per profili**
  Questa procedura è consigliata quando si desidera controllare regolarmente alcune directory e drive (ad esempio la propria directory di lavoro o drive, sui quali si archiviano regolarmente nuovi file). Queste directory e drive non devono quindi essere selezionati a ogni scansione ma vengono comodamente selezionati tramite il profilo corrispondente. Vedere Scansione diretta per profili.
- **Scansione diretta con il pianificatore**
  Il pianificatore offre la possibilità di far eseguire job temporizzati di scansione. Vedere Scansione diretta con il pianificatore.

Durante la scansione per rootkit, virus del record di avvio e la scansione dei processi attivi sono necessari dei procedimenti particolari. Sono disponibili le seguenti opzioni:

- Scansione di rootkit mediante il profilo di ricerca *Scansione alla ricerca di rootkit e malware attivi*
- Scansione dei processi attivi mediante il profilo di ricerca *Processi attivi*
- Scansiona virus del record di avvio con il comando **Scansiona virus del record di avvio** nel menu **Extra**

6. Aggiornamenti

L'efficacia di un software antivirus dipende dall'aggiornamento del programma, in particolare del file di definizione dei virus e del motore di ricerca. Per l'esecuzione degli aggiornamenti, il componente Updater è integrato nel prodotto Avira. Updater garantisce che il prodotto Avira sia sempre il più aggiornato possibile e che sia in grado di rilevare i nuovi virus che compaiono quotidianamente. Updater aggiorna i seguenti componenti:

- File di definizione dei virus:

  Il file di definizione dei virus contiene il modello di rilevamento del programma dannoso che il prodotto Avira utilizza nella scansione per virus e malware nonché nella riparazione di oggetti infetti.

- Motore di ricerca:

  Il motore di ricerca contiene i metodi che vengono utilizzati dal prodotto Avira per la scansione per virus e malware.

- File di programma (aggiornamento del prodotto):

  I pacchetti di aggiornamento del prodotto mettono a disposizione ulteriori funzioni per i singoli componenti del programma.

Durante un aggiornamento viene verificato lo stato di aggiornamento del file di definizione dei virus, dei file di programma e del motore di ricerca e, se necessario, tali componenti vengono aggiornati. Terminato un aggiornamento del prodotto può essere necessario riavviare il sistema. Se l'aggiornamento avviene solo per il file di definizione dei virus e per il motore di ricerca, non è necessario riavviare il computer.

Se dovesse essere necessario un riavvio dopo un aggiornamento del prodotto, è possibile decidere se proseguire con l'aggiornamento o se si preferisce ricevere un promemoria successivamente. Se si decide di proseguire con l'aggiornamento, è tuttavia possibile stabilire quando debba avvenire il riavvio.

Se si decide di effettuare l'aggiornamento in un momento successivo, vengono comunque aggiornati il file delle definizioni antivirus e il motore di ricerca, ma non i file di programma.

> **Nota**
> L'aggiornamento del prodotto non si completa fino a quando non è stato effettuato il riavvio.
>
> **Nota**
> Per motivi di sicurezza, Updater verifica se il file host di Windows del computer è stato modificato, ad esempio con manipolazione da parte di malware dell'URL di aggiornamento a seguito della quale Updater viene indirizzato a pagine di download indesiderate. Se il file host di Windows è stato manipolato, l'evento viene riportato nel file di record di Updater.

Viene automaticamente eseguito un aggiornamento con il seguente intervallo: 6 Ore.

In Control Center in **Pianificatore** è possibile configurare ulteriori job di aggiornamento che Updater deve eseguire a intervalli definiti. È inoltre possibile avviare l'aggiornamento manualmente:

- In Control Center: nel menu **Aggiornamento** e dalla rubrica **Stato**
- Tramite il menu contestuale dell'icona Tray

Gli aggiornamenti vengono richiamati da Internet tramite un server Web del produttore. Normalmente si utilizza la connessione di rete esistente per collegarsi al server di download di Avira. Questa impostazione standard può essere modificata nella configurazione in Configurazione > Aggiorna.

7. Risoluzione di problemi, suggerimenti

In questo capitolo vengono riportati accorgimenti importanti per la risoluzione dei problemi e altri consigli per la gestione del prodotto Avira.

- Vedere capitolo Assistenza in caso di problemi
- Vedere capitolo Shortcut
- Vedere capitolo Centro sicurezza di Windows (per Windows XP e Vista) o Centro operativo di Windows (a partire da Windows 7)

7.1 Assistenza in caso di problemi

Qui sono reperibili informazioni sulle cause e le soluzioni di eventuali problemi.

- Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file...* viene visualizzato nel tentativo di avviare un aggiornamento.
- Impossibile spostare o eliminare virus e malware.
- L'icona Tray mostra uno stato disattivato.
- Il computer diventa estremamente lento se eseguo un backup.
- Il Firewall segnala Avira Real-Time Protection , non appena è attivo.
- La chat Web non funziona: i messaggi di chat non vengono visualizzati.

Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file...* viene visualizzato nel tentativo di avviare un aggiornamento.

Causa: la connessione Internet non è attiva. Non è pertanto possibile creare un collegamento con il server Web su Internet.

- Provare se altri servizi Internet come WWW o l'e-mail funzionano. Se non funzionano ripristinare la connessione Internet.

Causa: il server proxy non è raggiungibile.

- Verificare se sia cambiato il login per il server proxy e adattare eventualmente la propria configurazione.

Causa: il file update.exe non è ammesso dal proprio firewall.

- Assicurarsi che il file update.exe sia ammesso dal proprio firewall.

Altrimenti:

- Controllare la configurazione (modalità esperto) dal percorso Sicurezza del computer > Aggiorna.

Impossibile spostare o eliminare virus e malware.

Causa: il file è stato caricato da Windows ed è attivo.

- Aggiornare il prodotto Avira.
- Se si utilizza il sistema operativo Windows XP, disattivare il ripristino del sistema.
- Avviare il computer in modalità provvisoria.
- Aprire la configurazione del prodotto Avira (modalità esperto).
- Selezionare **System Scanner > Scansione**, nel campo *File* attivare l'opzione **Tutti i file** e confermare facendo clic su **OK**.
- Avviare una scansione su tutti i drive locali.
- Avviare il computer in modalità normale.
- Eseguire una scansione in modalità normale.
- Se non vengono rilevati altri virus e malware attivare il ripristino del sistema se è disponibile e deve essere utilizzato.

L'icona Tray mostra uno stato disattivato.

Causa: il servizio Real-Time Protection è stato disattivato.

- Fare clic in Control Center sulla voce **Stato** e nel riquadro *Sicurezza del computer* attivare **Real-Time Protection**.

 - OPPURE -

- Fare clic con il tasto destro del mouse sull'icona Tray. Apparirà un menu contestuale. Fare clic su **Attiva Real-Time Protection**.

Causa: Avira Real-Time Protection viene bloccato dal firewall.

- Definire nella configurazione del firewall un permesso generale per Avira Real-Time Protection. Avira Real-Time Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet.

Altrimenti:

- Verificare la modalità di attivazione del servizio Avira Real-Time Protection. Eventualmente attivare il servizio: fare clic su **Start > Impostazioni >Pannello di controllo**. Fare doppio clic sulla finestra di configurazione **Servizi** per attivarla (in Windows XP l'applet dei servizi si trova nella sottocartella *Strumenti di amministrazione*). Cercare la voce *Avira Real-Time Protection*. Come modalità di avviamento deve essere inserito `Automatico` e come stato `Avviato`. Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante **Avvia**. Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi.

Il computer diventa estremamente lento se si esegue un backup.

Causa: Avira Real-Time Protection scansiona tutti i file con i quali lavora il sistema di backup durante il processo di backup.

- Selezionare nella configurazione (modalità esperto) **Real-Time Protection > Scansione > Eccezioni** e inserire i nomi di processo dei software di backup.

Il Firewall segnala Avira Real-Time Protection, non appena è attivo.

Causa: Avira Real-Time Protection comunicano tramite il protocollo Internet TCP/IP. Un firewall monitora tutte le connessioni mediante questo protocollo.

- Definire un permesso generale per Avira Real-Time Protection. Avira Real-Time Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet.

> **Nota**
> Si consiglia di eseguire regolarmente gli aggiornamenti Microsoft per colmare le eventuali lacune in termini di sicurezza.

La chat Web non funziona: i messaggi di chat non vengono visualizzati.

Questo fenomeno può verificarsi in chat che si basano sul protocollo HTTP con 'transfer-encoding= chunked'.

Causa: Web Protection controlla i dati inviati in modo completo alla ricerca di virus e programmi indesiderati prima che i dati siano caricati nel browser Web. Durante un trasferimento di dati con 'transfer-encoding= chunked', Web Protection non è in grado di rilevare la lunghezza dei messaggi o la quantità di dati.

- Nella configurazione impostare l'URL di Webchat come eccezione (vedere Configurazione: Web Protection > Scansione > Eccezioni).

7.2 Shortcut

Le shortcut offrono la possibilità di navigare velocemente nel programma, richiamare singoli moduli e avviare azioni.

Di seguito viene presentata una panoramica delle shortcut presenti disponibili. Per maggiori informazioni sulla funzionalità e disponibilità consultare il capitolo corrispondente della guida.

7.2.1 Nelle finestre di dialogo

Shortcut	Descrizione
Ctrl + Tab **Ctrl + Pggiù**	Navigazione in Control Center Passa alla rubrica successiva.
Ctrl + Maiusc + Tab **Ctrl + Pggiù**	Navigazione in Control Center Passa alla rubrica precedente.
←↑→↓	Navigazione nelle rubriche di configurazione Evidenzia con il mouse una rubrica di configurazione. Effettua una modifica tra le opzioni di un menu a tendina selezionate o tra più opzioni in un gruppo di opzioni.
Tab	Passa all'opzione successiva o al successivo gruppo di opzioni.
Maiusc + Tab	Passa all'opzione precedente o al precedente gruppo di opzioni.
Barra spaziatrice	Attiva o disattiva una casella di controllo se l'opzione attiva è una casella di controllo.
Alt + lettera sottolineata	Seleziona l'opzione o esegue il comando.
Alt + ↓ **F4**	Apre il menu a tendina selezionato.
Esc	Chiude il menu a tendina selezionato. Annulla il comando e chiude la finestra di dialogo.
Invio	Esegue comando per l'opzione o il pulsante attivo.

7.2.2 Nella Guida in linea

Shortcut	Descrizione
Alt + barra spaziatrice	Visualizza il menu del sistema.
Alt + Tab	Passa dalla Guida in linea ad altre finestre aperte.
Alt + F4	Chiude la Guida in linea.
Maiusc+ F10	Visualizza i menu contestuali della Guida in linea.
Ctrl + Tab	Passa alla rubrica successiva nella finestra di navigazione.
Ctrl + Maiusc + Tab	Passa alla rubrica precedente nella finestra di navigazione.
Pgsu	Passa all'argomento che è visualizzato sopra l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Pggiù	Passa all'argomento che è visualizzato sotto l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Pgsu **Pggiù**	Sfoglia le voci su un argomento.

7.2.3 In Control Center

Generale

Shortcut	Descrizione
F1	Visualizza la Guida in linea
Alt + F4	Chiude Control Center

F5	Aggiorna la visualizzazione
F8	Apre la configurazione
F9	Avvia aggiornamento

Rubrica **System Scanner**

Shortcut	Descrizione
F3	Avvia la scansione con il profilo selezionato
F4	Crea un collegamento sul desktop per il profilo selezionato

Rubrica **Quarantena**

Shortcut	Descrizione
F2	Scansiona nuovamente l'oggetto
F3	Ripristina l'oggetto
F4	Invia l'oggetto
F6	Ripristina l'oggetto in...
Invio	Proprietà
Agg	Aggiungi file
Canc	Elimina l'oggetto

Rubrica **Pianificatore**

Shortcut	Descrizione
F2	Modifica job
Invio	Proprietà
Agg	Inserisci nuovo job
Canc	Elimina job

Rubrica **Report**

Shortcut	Descrizione
F3	Visualizza il file di report
F4	Stampa il file di report
Invio	Mostra il report
Canc	Elimina il report

Rubrica **Eventi**

Shortcut	Descrizione
F3	Esporta eventi
Invio	Mostra evento
Canc	Elimina evento

7.3 Centro sicurezza PC di Windows

- a partire da Windows XP Service Pack 2 -

7.3.1 Generale

Il Centro sicurezza PC di Windows verifica lo stato di un computer dal punto di vista della sicurezza.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro sicurezza PC invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer.

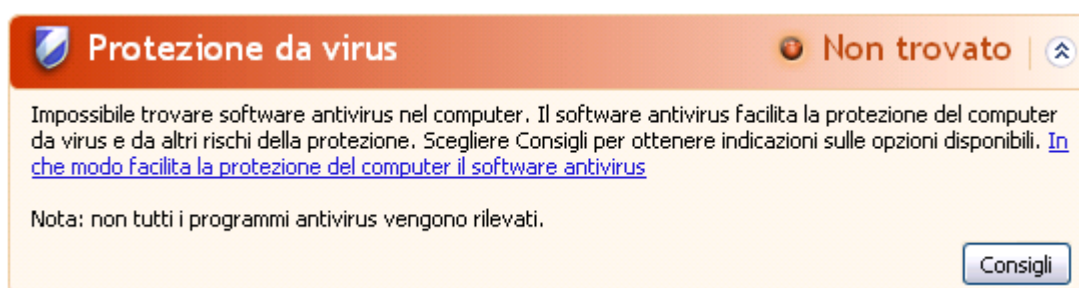
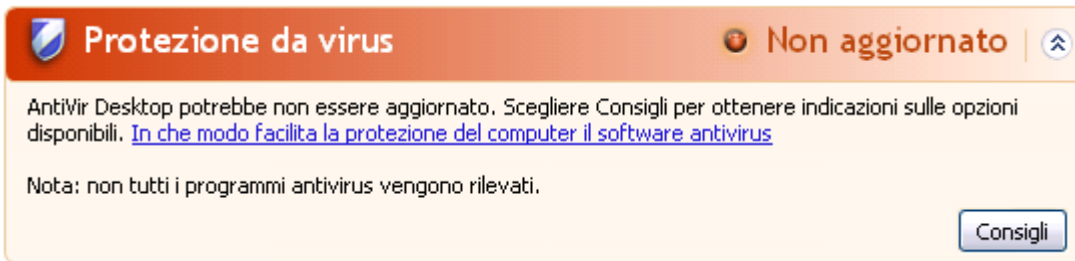
7.3.2 Centro sicurezza PC di Windows e il prodotto Avira in uso

Software di protezione antivirus/Protezione da software dannoso

È possibile ricevere i seguenti avvisi dal Centro sicurezza PC di Windows in relazione alla protezione antivirus.

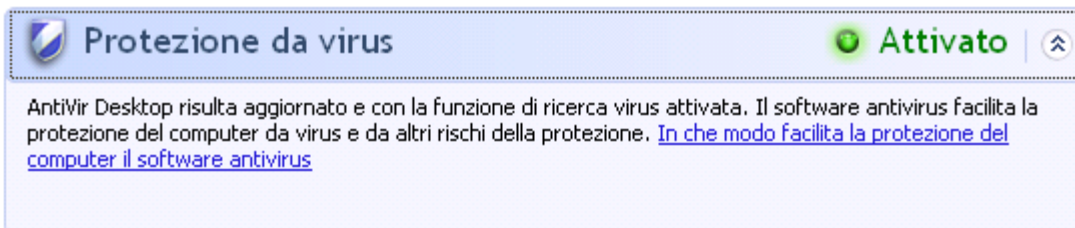
- Protezione antivirus NON TROVATA
- Protezione antivirus NON AGGIORNATA
- Protezione antivirus ATTIVA
- Protezione antivirus INATTIVA
- Protezione antivirus NON MONITORATA

Protezione antivirus NON TROVATA

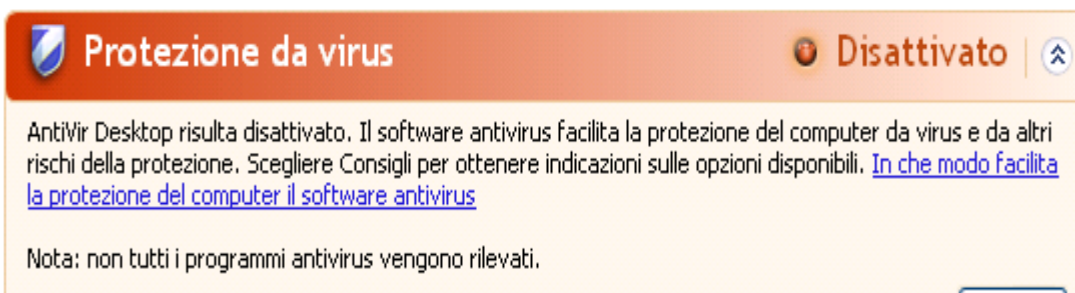
Questo avviso del Centro sicurezza PC di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

> **Nota**
> Installare sul computer il prodotto Avira in uso per proteggerlo da virus e altri programmi indesiderati!

Protezione antivirus NON AGGIORNATA

Se si possiede Windows XP Service Pack 2 o Windows Vista e si installa successivamente il prodotto Avira oppure si installa Windows XP Service Pack 2 o

Windows Vista su un sistema su cui il prodotto Avira è già installato, si riceve il seguente messaggio:

Nota
Per far sì che il Centro sicurezza PC di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Protezione antivirus ATTIVA

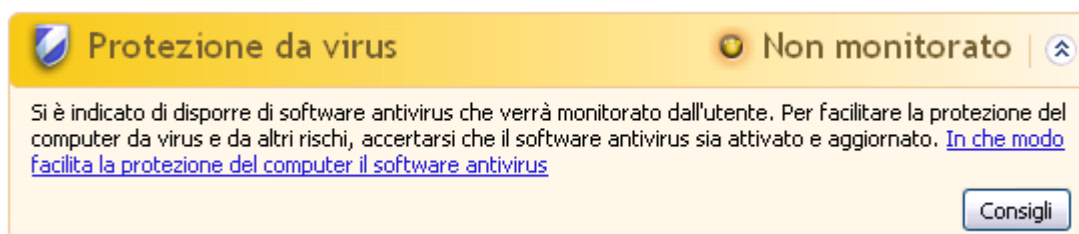
Dopo l'installazione del prodotto Avira e un successivo aggiornamento si riceve la seguente nota:

Il prodotto Avira ora è aggiornato e Avira Real-Time Protection è attivo.

Protezione antivirus INATTIVA

Si riceve la seguente nota se si disattiva Avira Real-Time Protection o si arresta il servizio Real-Time Protection.

Nota
Avira Real-Time Protection può essere attivato o disattivato dalla rubrica **Stato** di **Control Center**. Inoltre Real-Time Protection viene riconosciuto come attivato quando è aperto l'ombrellino rosso nella barra delle applicazioni.

Protezione antivirus NON MONITORATA

Si riceve il seguente messaggio dal Centro sicurezza PC di Windows poiché si è optato per l'automonitoraggio del software antivirus.

Nota
La funzione non è supportata da Windows Vista.

Nota
Il Centro sicurezza PC di Windows è supportato dal prodotto Avira in uso. È possibile attivare questa opzione in ogni momento con il pulsante **Consigli...**.

Nota
Anche se si possiede Windows XP Service Pack 2 o Windows Vista installati si ha comunque bisogno di una soluzione antivirus . Sebbene Windows controlli il software antivirus non ha alcuna funzione antivirus. L'utente non sarebbe protetto contro virus e malware senza una soluzione antivirus aggiuntiva!

7.4 Centro operativo di Windows

- Windows 7 e Windows 8 -

7.4.1 Generale

Nota:
il **Centro sicurezza PC di Windows** da Windows 7 ha assunto il nome **Centro operativo di Windows**. Questa parte del programma indica lo stato di tutte le opzioni di sicurezza.

Il Centro operativo di Windows verifica lo stato di un computer dal punto di vista della sicurezza. È possibile accedere direttamente al Centro operativo facendo clic sulla bandierina nella barra delle applicazioni oppure su **Pannello di controllo > Centro operativo**.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro operativo invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer. Ciò significa che, se tutto funziona correttamente, il Centro operativo non invia nessun avviso. È possibile tuttavia controllare lo stato di sicurezza del computer nel **Centro operativo** nella rubrica **Sicurezza**.
È possibile gestire e selezionare i programmi installati (ad esempio *visualizzare i programmi anti-spyware sul computer*).

Da **Centro operativo > Modifica impostazioni** è possibile disattivare i messaggi di avviso (ad esempio *Disattivazione dei messaggi per la sicurezza relativi a spyware e malware simili*).

7.4.2 Centro operativo di Windows e il prodotto Avira in uso

Protezione antivirus

È possibile ricevere i seguenti avvisi dal Centro operativo di Windows in relazione alla protezione antivirus:

- Avira Desktop ha segnalato che è installata la versione più recente e il riconoscimento dei virus è attivo
- Avira Desktop è disattivato
- Avira Desktop non è aggiornato
- Impossibile trovare software antivirus installato nel computer
- Avira Desktop non protegge più il PC

Avira Desktop ha segnalato che la versione installata è la più recente e il riconoscimento dei virus è attivo

Dopo l'installazione del prodotto Avira e un successivo aggiornamento non viene visualizzato nessun messaggio dal Centro operativo di Windows. In **Centro operativo > Sicurezza** può comparire il seguente messaggio: *"Avira Desktop" ha segnalato che la versione installata è la più recente e il riconoscimento dei virus è attivo*. Questo significa che il prodotto Avira ora è aggiornato e Avira Realtime Protection è attivo.

Avira Desktop è disattivato

Il seguente messaggio viene visualizzato se si disattiva Avira Realtime Protection o si arresta il servizio Realtime Protection.

Protezione da virus (Importante)
Avira Desktop è disattivato.
Disattiva i messaggi relativi a: protezione da virus
Attiva ora
Recuperare un altro programma antivirus online

> **Nota**
> **Avira Realtime Protection** può essere attivato o disattivato dalla rubrica **Stato** di **Avira Control Center**. Inoltre si può riconoscere se **Avira Realtime Protection** è attivo quando l'ombrellino rosso nella barra delle applicazioni è aperto. È possibile altresì attivare i singoli componenti di Avira facendo clic sul pulsante *Attiva ora* del Centro operativo. Se viene visualizzato un messaggio che richiede l'autorizzazione all'esecuzione del programma Avira, fare clic su *Consenti* per attivare Realtime Protection.

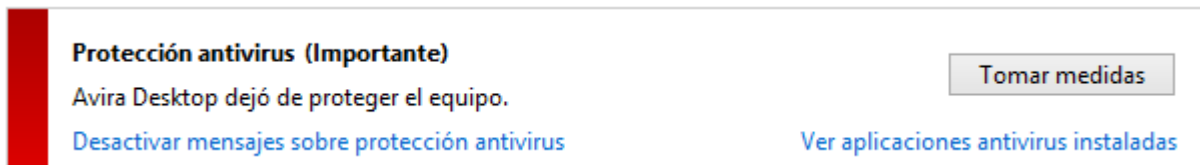
Avira Desktop non è aggiornato

Se avete appena installato Avira o se un qualche motivo il file della definizione antivirus, il motore di ricerca o i file di programma del vostro prodotto Avira non sono stati aggiornati automaticamente, (ad es. se da una vecchia versione del sistema operativo Windows su cui era già installato il vostro prodotto Avira passate ad una nuova versione), è visualizzato il seguente avviso:

> **Nota**
> Per far sì che il Centro operativo di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Impossibile trovare software antivirus installato nel computer

Questo avviso del Centro operativo di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

> **Nota**
> Attenzione: questa opzione non è disponibile per Windows 8. Windows Defender a partire da questo sistema operativo è la funzione antivirus preimpostata di Microsoft.
>
> **Nota**
> Installare sul computer il prodotto Avira in uso per proteggerlo da virus e altri programmi indesiderati!

Avira Desktop non protegge più il PC

Questa nota del centro operativo Windows compare quando la licenza del vostro prodotto Avira è scaduta.
Facendo clic sul pulsante **Esegui azione** si viene indirizzati al sito Web di Avira, dove è possibile acquistare una nuova licenza.

> **Nota**
> Attenzione: questa opzione è disponibile solo per Windows 8.

Protezione da spyware e software indesiderati

È possibile ricevere i seguenti avvisi dal Centro operativo di Windows in relazione alla protezione da spyware e software indesiderati:

- Avira Desktop ha segnalato che è attivo
- Sia il Defender Windows, sia il desktop Avira hanno segnalato di essere non attivi
- Avira Desktop non è aggiornato
- Windows Defender non è aggiornato
- Windows Defender è disattivato

Avira Desktop ha segnalato che è attivo

Dopo l'installazione del prodotto Avira e un successivo aggiornamento non viene visualizzato nessun messaggio dal Centro operativo di Windows. In **Centro operativo > Sicurezza** può comparire il seguente messaggio: *"Avira Desktop" ha segnalato che è attivo*. Questo significa che il prodotto Avira ora è aggiornato e Avira Realtime Protection è attivo.

Sia il Defender Windows, sia il desktop Avira hanno segnalato di essere non attivi

Il seguente messaggio viene visualizzato se si disattiva Avira Realtime Protection o si arresta il servizio Avira Realtime Protection.

Spyware e protezione da software indesiderato (Importante)
Windows Defender e Avira Desktop sono disattivati.
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Visualizza programmi antispywa...

> **Nota**
> **Avira Realtime Protection** può essere attivato o disattivato dalla rubrica **Stato** di **Avira Control Center**. Inoltre si può riconoscere se **Avira Realtime Protection** è attivo quando l'ombrellino rosso nella barra delle applicazioni è aperto. È possibile altresì attivare i singoli componenti di Avira facendo clic sul pulsante *Attiva ora* del Centro operativo. Se viene visualizzato un messaggio che richiede l'autorizzazione all'esecuzione del programma Avira, fare clic su *Consenti* per attivare Realtime Protection.

Avira Desktop non è aggiornato

Se avete appena installato Avira o se per un qualche motivo il file delle definizioni antivirus, il motore di ricerca o i file di programma del vostro prodotto Avira non sono stati aggiornati automaticamente, (ad es. se da una vecchia versione del sistema operativo Windows su cui era già installato il prodotto Avira si passa ad una nuova versione), è visualizzato il seguente avviso:

> **Nota**
> Per far sì che il Centro operativo di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Windows Defender non è aggiornato

Il seguente messaggio viene visualizzato se Windows Defender è attivo. Ciò potrebbe significare che il prodotto Avira in uso non è stato installato correttamente. Controllare.

Spyware e protezione da software indesiderato (Importante)

Windows Defender non è aggiornato.

Aggiorna

Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati

Recuperare un altro programma antispyware online

Nota
Windows Defender è la soluzione anti-spyware e antivirus predefinita di Windows.

Windows Defender è disattivato

Il messaggio del Centro operativo di Windows *Windows Defender è disattivato* viene visualizzato se sul computer non sono stati trovati altri software anti-spyware. Windows Defender è un software per il riconoscimento degli spyware di Microsoft integrato nel sistema operativo. Se sul computer è già stato installato un altro software antivirus, quest'applicazione viene disattivata.
Se il prodotto Avira è installato correttamente questo messaggio non dovrebbe comparire, perché il Centro operativo riconosce automaticamente Avira. Controllare se Avira funziona correttamente.

8. Virus e altro

8.1 Virus e altro

Avira Free Antivirus non si limita al riconoscimento di virus e malware, ma può anche proteggere da altri rischi. In questo capitolo viene presentata una panoramica dei diversi tipi di malware e degli altri rischi. Viene descritta la loro provenienza e il loro comportamento, nonché le spiacevoli sorprese che possono causare.

Argomenti correlati:

- Categorie di minacce
- Virus e altri malware

8.2 Categorie di minacce

Adware

Con Adware si designa un software che mostra all'utente i banner e i popup pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Il prodotto Avira riconosce gli adware. Se nella configurazione in Categorie di minacce l'opzione **Adware** è attivata, si riceve un avviso quando il prodotto Avira rileva un software di questo tipo.

Adware/Spyware

Software che visualizza messaggi pubblicitari o che invia i dati personali dell'utente, spesso a sua insaputa, a terzi e che risulta quindi indesiderato.

Il prodotto Avira riconosce gli Adware/Spyware. Se nella configurazione in Categorie di minacce l'opzione **Adware/Spyware** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira esegue un rilevamento.

Applicazione

Per applicazione si intende un'applicazione il cui utilizzo può essere rischioso o la cui origine è dubbia.
Il prodotto Avira riconosce l'Applicazione (APPL). Se nella configurazione in Categorie di minacce l'opzione **Applicazione** è attivata con un segno di spunta, si riceve un avviso se il prodotto Avira effettua un rilevamento.

Software di controllo backdoor

Per prelevare dati o manipolare il sistema viene inserito dalla porta posteriore un programma server backdoor senza che l'utente se ne accorga. Questo programma può essere gestito da terzi mediante Internet o la rete con un software di gestione backdoor (Client).
Il prodotto Avira riconosce i software di controllo backdoor. Se nella configurazione in Categorie di minacce l'opzione **Software di controllo backdoor** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira esegue un rilevamento.

File con estensioni occultate

File eseguibili che occultano la propria estensione in modo sospetto. Il metodo dell'occultamento viene spesso utilizzato dai malware.
Il prodotto Avira riconosce i file con estensioni occultate. Se nella configurazione in Categorie di minacce l'opzione **File con estensioni occultate** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programma di selezione a pagamento

Alcuni servizi offerti in Internet sono a pagamento. In Germania la fatturazione avviene per programmi di selezione con i numeri 0190/0900 (in Austria e Svizzera con i numeri 09x0; in Germania a medio termine passerà ai numeri 09x0). Se installati sul computer, questi programmi (dialer) garantiscono la creazione della connessione mediante i numeri Premium-Rate, la cui tariffa può variare enormemente.

La commercializzazione di contenuti online mediante la bolletta telefonica è legale e può essere vantaggiosa per l'utente. I dialer seri non hanno alcun dubbio sul fatto che il cliente sia consapevole e lo utilizzi in modo avveduto. Tali contenuti si installano sul computer dell'utente solo se l'utente dà la propria approvazione, espressa sulla base di un'etichettatura ben riconoscibile o di una richiesta univoca e chiara. La creazione della connessione di programmi dialer seri viene visualizzata in maniera chiara e non ambigua. Inoltre, i dialer seri informano l'utente in maniera esatta e precisa sui costi correlati.

Purtroppo però esistono dialer che si installano senza farsi notare, in maniera dubbia o addirittura fraudolenta. Sostituiscono, ad esempio, la connessione standard dial up dell'utente di Internet all'ISP (Internet-Service-Provider) e a ogni connessione selezionano numeri a pagamento spesso estremamente costosi, come i numeri 0190/0900. L'utente interessato nota dalla bolletta successiva che è stato installato un programma dialer indesiderato che si connette a ogni accesso a Internet ai numeri a pagamento 0190/0900, facendo salire in modo esorbitante la bolletta.

Per proteggersi da programmi di selezione non desiderati e a pagamento (dialer 0190/0900), consigliamo di rivolgersi direttamente al proprio gestore telefonico per bloccare questo tipo di numeri.

Di default, il prodotto Avira riconosce i programmi di selezione a pagamento a lui noti.

Se nella configurazione di Categorie di minacce è stata attivata l'opzione **Programmi di selezione a pagamento** con un segno di spunta, in caso di rilevamento di un programma di selezione a pagamento viene emesso un messaggio di avviso. Si ha quindi la possibilità di eliminare facilmente gli eventuali dialer indesiderati per i numeri 0190/0900. Se si tratta di un programma di selezione a pagamento voluto, si può dichiarare un file da escludere che non verrà più scansionato in futuro.

Phishing

Il phishing, anche noto come brand spoofing è una forma raffinata di furto dei dati per i clienti o i potenziali clienti di provider Internet, banche, servizi di banking online, enti di registrazione.
Con la trasmissione dell'indirizzo e-mail in Internet, la compilazione di moduli online, la partecipazione a newsgroup o siti Web, è possibile che vengano sottratti i dati dai cosiddetti Internet crawling spiders e utilizzati senza autorizzazione per frodi o altre attività illegali.

Il prodotto Avira riconosce il phishing. Se nella configurazione in Categorie di minacce l'opzione **Phishing** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programmi che violano la privacy dell'utente

Software che minano la sicurezza del sistema, causano funzioni di programma non desiderate, violano la sfera privata o spiano il comportamento dell'utente e che sono quindi generalmente indesiderati.

Il prodotto Avira riconosce i software che mettono a repentaglio la sicurezza. Se nella configurazione in Categorie di minacce l'opzione **Programmi che violano la privacy dell'utente** è attivata con un segno di spunta, si riceve un avviso se il prodotto Avira ha eseguito un rilevamento.

Programmi ludici

I programmi ludici possono inorridire qualcuno o divertire tutti, senza essere dannosi o moltiplicarsi. La maggior parte delle volte il computer dopo il richiamo del programma ludico inizia a far suonare una melodia o a visualizzare qualcosa di insolito sullo schermo. Esempi di programmi ludici sono le lavatrici nel drive del floppy disk (DRAIN.COM) o il divoraschermo (BUGSRES.COM).

Ma attenzione! Tutte le manifestazioni di un programma ludico potrebbero anche essere prodotte da un virus o un trojan. L'effetto minimo sull'utente è uno spavento ma si può anche andare nel panico per la paura dei danni che possono verificarsi.

Il prodotto Avira è in grado di riconoscere i programmi ludici mediante un'estensione delle proprie routine di scansione ed eventualmente di eliminare il programma indesiderato. Se nella configurazione in Categorie di minacce è stata selezionata l'opzione **Programmi ludici** con un segno di spunta, si viene informati sui relativi rilevamenti.

Giochi

I giochi per computer devono esistere, ma non necessariamente sul luogo di lavoro (ad eccezione a volte della pausa pranzo). Tuttavia i dipendenti delle aziende e i collaboratori degli enti pubblici spesso usano i giochi. Su Internet sono disponibili moltissimi giochi. Anche i giochi tramite e-mail stanno prendendo piede: dal semplice gioco degli scacchi a battaglia navale (con tanto di battaglie con torpedo), sono numerose le varianti in circolazione. Le mosse vengono inviate e ricevute mediante il programma di posta elettronica.

Alcune ricerche hanno dimostrato che il tempo durante l'orario lavorativo dedicato ai giochi per computer sta assumendo proporzioni rilevanti. Pertanto è comprensibile che sempre più aziende prendano in considerazione la possibilità di eliminare i giochi dai computer utilizzati per lavoro.

Il prodotto Avira riconosce i giochi per computer. Se nella configurazione in Categorie di minacce l'opzione **Giochi** è attivata con un segno di spunta, si riceve un avviso se il prodotto Avira ha eseguito un rilevamento. Il gioco è finito nel vero senso della parola visto che è possibile escluderlo facilmente.

Software ingannevole

Noti anche con il nome di Scareware (programmi spaventosi) o Rogueware (programmi canaglia), sono software ingannevoli che simulano infezioni di virus e rischi e quindi sono ingannevolmente simili ai software antivirus professionali. Gli scareware mirano a disorientare o spaventare l'utente. Se la vittima cade nel trabocchetto e si sente minacciata, gli viene offerta una soluzione (spesso a pagamento) per rimuovere la minaccia inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile l'attacco vero e proprio.

Se nella configurazione di Categorie di minacce è stata attivata l'opzione **Software ingannevole** con un segno di spunta, in caso di rilevamento di uno scareware viene emesso un messaggio di avviso.

Programmi di compressione runtime insoliti

I file compressi con un programma di compressione runtime insolito possono essere identificati come sospetti.

Il prodotto Avira riconosce gli strumenti di compressione runtime insoliti. Se nella configurazione in Categorie di minacce l'opzione **Strumento di compressione runtime insolito** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

8.3 Virus e altri malware

Adware

Con Adware si designa un software che mostra all'utente i banner e i popup pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Backdoor

Un backdoor (in italiano porta posteriore) permette, aggirando la tutela all'accesso, di ottenere l'accesso a un computer.

Un programma in esecuzione di nascosto permette a un aggressore di godere di diritti pressoché illimitati. Con l'aiuto del backdoor i dati personali dell'utente possono essere spiati. I backdoor però vengono utilizzati soprattutto per installare altri virus o worm sul sistema infetto.

Virus dei record di avvio

Il record di avvio e il record master di avvio degli hard disk vengono inficiati di preferenza da virus dei record di avvio, che sovrascrivono informazioni importanti all'avvio del sistema. Una delle spiacevoli conseguenze è che il sistema operativo non può più essere caricato...

Bot-Net

Per Bot-Net si intende una rete di PC gestibile a distanza (in Internet), composta da bot che comunicano l'uno con l'altro. Questo controllo si raggiunge con virus e trojan che inficiano il computer e poi aspettano indicazioni senza apportare danni al computer intaccato. Queste reti possono essere utilizzare per la diffusione di spam, attacchi DDoS, ecc., talvolta senza che gli utenti del PC si accorgano di alcunché. Il potenziale principale dei Bot-Net è quello di poter raggiungere reti di migliaia di computer, la cui portata salta gli accessi a Internet.

Exploit

Un Exploit (lacuna di sicurezza) è un programma del computer o uno script che sfrutta le debolezze specifiche o le funzioni errate di un sistema operativo o del programma. Una forma di Exploit sono gli attacchi da Internet con l'aiuto di pacchetti di dati manipolati, che sfruttano le debolezze nel software di rete. Con l'utilizzo di alcuni programmi che si introducono clandestinamente si ottiene un più ampio accesso.

Hoaxes (in inglese hoax: scherzo, burla)

Da un paio di anni gli utenti ricevono avvisi di virus che potrebbero diffondersi per e-mail in Internet o in altre reti. Questi avvisi vengono distribuiti via e-mail con la richiesta di inoltrarli a quanti più colleghi possibili per mettere tutti in guardia dal "pericolo".

Honeypot

Un Honeypot (pentola di miele) è un servizio installato in una rete (programma o server). Esso ha il compito di monitorare una rete e registrare gli attacchi. Questo servizio è sconosciuto all'utente legittimo e quindi non viene mai toccato. Quando un aggressore cerca punti di debolezza in una rete e prende in considerazione i servizi offerti da un Honeypot, viene registrato e viene emesso un allarme.

Macrovirus

I macrovirus sono piccoli programmi che sono scritti nella lingua delle macro di un'applicazione (ad esempio WordBasic in WinWord 6.0) e normalmente potrebbero diffondersi all'interno di documenti di questa applicazione. Essi vengono pertanto chiamati anche virus dei documenti. Per renderli attivi è necessario avviare l'applicazione corrispondente ed eseguire una delle macro infette. Diversamente dai virus "normali", i macrovirus non riguardano i file eseguibili, bensì i documenti dell'applicazione host.

Pharming

Il pharming è una manipolazione del file host dei browser Web, per reindirizzare richieste dei siti Web falsificati. Si tratta di una rielaborazione del classico phishing. I truffatori che si servono del pharming godono di grandi quantità di server sui quali vengono archiviati i siti Web falsificati. Il pharming si è consolidato come iperonimo per diversi tipi di attacchi al DNS. In caso di manipolazione del file host con l'ausilio di un trojan o un virus viene effettuata una manipolazione del sistema. La conseguenza è che sono richiamabili solo siti Web falsificati da questo sistema, se l'indirizzo Web viene inserito correttamente.

Phishing

Phishing significa letteralmente pescare dati personali degli utenti di Internet. Il phisher invia generalmente alla vittima lettere aventi valore ufficiale, come ad esempio e-mail che veicolano informazioni sensibili, soprattutto nomi utente e password o PIN e TAN di accessi all'Online Banking, approfittando della buona fede dell'utente. Con i dati di accesso rubati il phisher assume l'identità della vittima e conduce operazioni a suo nome. Va precisato che le banche e le assicurazioni non chiedono mai di inviare numeri di carte di credito, PIN, TAN o altri dati di accesso per e-mail, SMS o telefonicamente.

Virus polimorfi

I veri campioni del mimetismo e del travestimento sono i virus polimorfi. Modificano i propri codici di programmazione e sono quindi particolarmente difficili da riconoscere.

Virus di programma

Un virus del computer è un programma che ha la capacità, una volta richiamato, di agganciarsi in qualche modo ad altri programmi e, da tale posizione, di inficiare il sistema. I virus si diffondono quindi in contrasto alle bombe logiche e ai trojan stessi. Al contrario di un worm, un virus ha bisogno di un programma estraneo ospite in cui archiviare il proprio codice virulento. Normalmente, tuttavia, la funzionalità del programma ospite non viene modificata.

Rootkit

Per rootkit si intende un insieme di strumenti software che vengono installati su un computer dopo un'irruzione per nascondere il login dell'intruso, nascondere processi e registrare dati, in linea generale: per rendersi invisibili. I rootkit tentano di aggiornare i programmi spia già installati e di installare nuovamente gli spyware eliminati.

Virus di script e worm

Questi virus sono estremamente semplici da programmare e in poche ore si diffondono per e-mail a livello globale, premesso che siano presenti tecniche ad hoc.

I virus di script e i worm utilizzano la lingua degli script, come ad esempio Javascript, VBScript ecc., per inserirsi in altri nuovi script o per diffondersi mediante il richiamo di funzioni del sistema operativo. Spesso ciò avviene tramite e-mail o mediante lo scambio di file (documenti).

Il worm è un programma che non intacca alcun documento ospite. I worm non possono quindi divenire un componente di altri programmi. I worm rappresentano spesso l'unica possibilità di introdursi clandestinamente su sistemi dotati di provvedimenti restrittivi legati alla sicurezza.

Spyware

Gli spyware sono i cosiddetti programmi spia che inviano dati personali dell'utente a terzi senza che questi ne siano a conoscenza e senza l'approvazione del produttore del software. I programmi spyware servono soprattutto ad analizzare la navigazione in Internet e a introdurre banner o popup pubblicitari in maniera mirata.

Cavalli di Troia (in breve trojan)

I trojan sono sempre più diffusi. Così vengono definiti i programmi che pretendono di avere una funzione precisa; dopo il loro avvio, tuttavia, mostrano il loro vero volto ed eseguono altre funzioni che hanno per lo più effetti distruttivi. I trojan non possono moltiplicarsi da soli e in questo si differenziano dai virus e dai worm. La maggior parte di loro ha un nome interessante (SEX.EXE o STARTME.EXE), che ha la funzione di spingere l'utente a eseguire il trojan. Subito dopo l'esecuzione diventano attivi e formattano, ad esempio, l'hard disk. Un tipo particolare di trojan è il dropper, che "lascia cadere" i virus, ovvero li installa nel sistema del computer.

Software ingannevole

Noti anche con il nome di Scareware (programmi spaventosi) o Rogueware (programmi canaglia), sono software ingannevoli che simulano infezioni di virus e rischi e quindi sono ingannevolmente simili ai software antivirus professionali. Gli scareware mirano a disorientare o spaventare l'utente. Se la vittima cade nel trabocchetto e si sente minacciata, gli viene offerta una soluzione (spesso a pagamento) per rimuovere la minaccia inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile l'attacco vero e proprio.

Zombie

Un PC zombie è un computer che viene intaccato da programmi malware e permette all'hacker di abusare del computer in remoto per fini criminali. Il PC infetto lancia il comando, ad esempio, di attacchi di Denial-of-Service- (DoS) o invia spam o e-mail di phishing.

9. Info e Service

In questo capitolo sono disponibili informazioni sui modi in cui è possibile tenersi in contatto con noi.

- vedere il capitolo Indirizzo di contatto
- vedere il capitolo Supporto tecnico
- vedere il capitolo File sospetto
- vedere il capitolo Segnalazione di un falso allarme

9.1 Indirizzi di contatto

Siamo a disposizione del cliente qualora avesse domande o suggerimenti sul mondo dei prodotti di Avira. I nostri recapiti sono disponibili in Control Center alla voce **Guida in linea > Informazioni su Avira Free Antivirus**.

9.2 Supporto tecnico

Il supporto Avira è rivolto all'utente, serve a rispondere alle sue domande o a risolvere un problema tecnico.

Sul nostro sito Web sono disponibili tutte le informazioni utili per accedere al nostro ampio servizio di supporto:
http://www.avira.it/personal-support

Per poter ricevere aiuto nel modo migliore e più veloce possibile, occorre tenere a portata di mano le seguenti informazioni:

- **Informazioni sulla versione**. Si trovano sull'interfaccia del programma nella voce di menu **Guida in linea > Informazioni su Avira Free Antivirus > Informazioni sulla versione**. Vedere Informazioni sulla versione.
- **Versione del sistema operativo** e service pack eventualmente installati.
- **I pacchetti software installati**, ad esempio software antivirus di altri produttori.
- **Messaggi precisi** del programma o del file di report.

9.3 File sospetto

I file sospetti o i virus che non possono essere riconosciuti o eliminati dai nostri prodotti possono essere inviati a noi. A tale scopo sono disponibili diverse modalità di invio.

- Selezionare il file nel Gestore della quarantena di Control Center e selezionare la voce **Invia file** mediante il menu contestuale o i pulsanti corrispondenti.

- Inviare il file desiderato in formato compresso (WinZIP, PKZip, Arj, ecc.) come allegato a un'e-mail al seguente indirizzo:
  virus-personal@avira.it
  Poiché alcuni gateway di posta elettronica operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

9.4 Comunicazione di un falso allarme

Se si ritiene che il prodotto Avira in uso abbia segnalato un rilevamento in un file che tuttavia con tutta probabilità è "pulito", si prega di inviare tale file compresso (WinZIP, PKZIP, Arj, ecc.) per e-mail come allegato al seguente indirizzo:
virus-personal@avira.it

Poiché alcuni gateway di posta elettronica operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

10. Riferimento: Opzioni di configurazione

Il riferimento della configurazione elenca tutte le opzioni di configurazione disponibili.

10.1 System Scanner

La rubrica **System Scanner** della configurazione è dedicata alla configurazione della scansione diretta, ovvero alla scansione su richiesta. Le opzioni sono disponibili solo se la modalità esperto è attiva.

10.1.1 Scansione

Qui si può definire la procedura standard della routine di scansione durante una scansione diretta (le opzioni sono disponibili solo se la modalità esperto è attiva). Se si seleziona una determinata directory da controllare durante la scansione diretta, System Scanner esegue i controlli in base alla configurazione:

- con una determinata prestazione di scansione (priorità),
- anche sui record di avvio e nella memoria principale,
- su tutti i file o i file selezionati nella directory.

File

System Scanner può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file indipendentemente dal contenuto e dall'estensione. Il filtro non viene utilizzato.

> **Nota**
> Se **Tutti i file** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il prodotto Avira decide, in base al contenuto di un file, se quest'ultimo deve essere controllato o meno per verificare la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza l'elenco delle estensioni**, ma molto più sicura poiché i controlli non vengono effettuati solamente sulla base delle estensioni dei file. Questa impostazione è attivata di default ed è consigliata.

> **Nota**
> Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza l'elenco delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file**".

> **Nota**
> Se questa opzione è attiva e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza l'elenco delle estensioni**". Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o rimuovere voci.

> **Nota**
> Prestare attenzione al fatto che l'elenco standard può variare da versione a versione.

Impostazioni aggiuntive

Scansiona settori di avvio dei drive

Se l'opzione è attivata, System Scanner controlla i record di avvio dei drive selezionati durante la scansione diretta. Questa impostazione è attivata di default.

Scansione dei record master di avvio

Se l'opzione è attivata, System Scanner controlla i record master di avvio degli/dell'hard disk utilizzati/o nel sistema.

Ignora i file offline

Se l'opzione è attivata, la scansione diretta ignora completamente i cosiddetti file offline durante la scansione. Ciò significa che in questi file non viene controllata la presenza di virus e programmi indesiderati. I file offline sono i file che sono stati archiviati fisicamente dall'hard disk, ad es. su un nastro, mediante il cosiddetto sistema gerarchico di gestione della memoria (HSM). Questa impostazione è attivata di default.

Controllo di integrità dei file di sistema

Se l'opzione è attivata, i principali file di sistema di Windows vengono sottoposti a una verifica particolarmente sicura durante ogni scansione diretta per verificare la presenza di modifiche dovute a malware. Se viene individuato un file modificato, questo viene segnalato come rilevamento sospetto. La funzionalità occupa molta memoria. Per questo motivo l'opzione è disattivata di default.

> **Nota**
> L'opzione è disponibile solo a partire da Windows Vista.

> **Nota**
> Se si utilizzano strumenti di terze parti, si modificano i file di sistema o si personalizza la schermata di avvio, questa opzione non deve essere utilizzata. Questi strumenti sono, ad esempio, i cosiddetti skinpack, TuneUp Utilities o Vista Customization.

Scansione ottimizzata

Se l'opzione è attivata, durante la scansione di System Scanner la capacità del processore viene utilizzata in modo ottimale. Per motivi di performance, in caso di scansione ottimale, la funzione di log si verifica al massimo a un livello standard.

> **Nota**
> L'opzione è disponibile solo per computer multiprocessore.

Seguire link simbolici

Se l'opzione è attivata, System Scanner esegue una scansione di tutti i collegamenti simbolici nel profilo di ricerca o nelle directory selezionate, allo scopo di scansionare i file collegati alla ricerca di virus e malware.

> **Nota**
> L'opzione non comprende i collegamenti (shortcut), bensì si riferisce esclusivamente ai link simbolici (generati con mklink.exe) o ai punti di giunzione (generati con junction.exe), presenti in modalità trasparente nel file system.

Scansione rootkit all'avvio

Se l'opzione è attivata, System Scanner verifica all'avvio della scansione la presenza di rootkit attivi nella directory di sistema Windows tramite una cosiddetta procedura rapida. Questa procedura non verifica se nel computer vi sono rootkit attivi così dettagliatamente come il profilo di ricerca "**Cerca Rootkits**", ma è molto più rapida.

Nota
Scansione rootkit in Windows XP a 64 bit non disponibile!

Scansiona registro

Se l'opzione è attivata, viene scansionato il registro alla ricerca di software dannosi.

Processo di scansione

Permetti l'arresto

Se l'opzione è attivata, la ricerca di virus o programmi indesiderati può essere arrestata in ogni momento con il pulsante "**Arresta**" nella finestra "**Luke Filewalker**". Se questa impostazione è disattivata, il pulsante **Arresta** nella finestra "**Luke Filewalker**" è grigio. Pertanto non è possibile terminare prematuramente una scansione. Questa impostazione è attivata di default.

Priorità del sistema di scansione

System Scanner differenzia tre livelli di priorità nella scansione diretta. Si tratta di un sistema efficace solo se sul computer sono in esecuzione più processi contemporaneamente. La scelta si ripercuote anche sulla velocità di scansione.

Livello basso

System Scanner riceve dal sistema operativo il tempo del processore solo se nessun altro processo necessita di tempo di elaborazione, ovvero finché il sistema di scansione è l'unico programma in esecuzione, la velocità è massima. Nel complesso, in questo modo viene gestito molto bene anche il lavoro con altri programmi: il computer è più veloce se altri programmi sono in esecuzione, mentre System Scanner lavora in background.

Livello medio

System Scanner viene eseguito con priorità normale. Tutti i processi ricevono lo stesso tempo di elaborazione dal sistema operativo. Questa impostazione è attivata di default ed è consigliata. In alcune circostanze il lavoro con altre applicazioni ne risulta compromesso.

Livello elevato

System Scanner riceve la massima priorità. Un lavoro parallelo con altre applicazioni è pressoché impossibile. Tuttavia System Scanner completa la scansione in maniera estremamente rapida.

Azione in caso di rilevamento

È possibile definire le azioni che System Scanner deve eseguire quando viene rilevato un virus o un programma indesiderato. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Interattivo

Se l'opzione è attivata, i rilevamenti della scansione di System Scanner vengono notificati in una finestra di dialogo. Al termine della scansione di System Scanner, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure arrestare System Scanner.

> **Nota**
> Di default nella finestra di dialogo è preselezionata l'azione **Quarantena**. È possibile selezionare ulteriori azioni mediante il menu contestuale.

Automatico

Se l'opzione è attivata, in caso di rilevamento di virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. System Scanner reagisce conformemente alle impostazioni definite precedentemente dall'utente in questa sezione.

Copia il file in quarantena prima dell'azione

Se l'opzione è attivata, System Scanner crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene mantenuta in quarantena dove il file può essere ripristinato se possiede un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center per ulteriori indagini.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando System Scanner rileva un virus o un programma indesiderato. Se l'opzione "**Ripara**" è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in "**Azione secondaria**".

> **Nota**
> L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

Ripara

Se l'opzione è attivata, System Scanner ripara automaticamente i file infetti. Se System Scanner non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

> **Nota**
> Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte di System Scanner.

Rinomina

Se l'opzione è attivata, System Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

Quarantena

Se l'opzione è attivata, System Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato.

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Azione secondaria

L'opzione "**Azione secondaria**" è selezionabile solo se in "**Azione primaria**" è stata selezionata l'impostazione **Ripara**. Con questa opzione si può decidere come procedere con il file infetto se non è riparabile.

Rinomina

Se l'opzione è attivata, System Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

Quarantena

Se l'opzione è attivata, System Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato.

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

> **Nota**
> Se si seleziona **Elimina** o come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati bensì spostati in quarantena.

Archivi

Per la ricerca negli archivi il System Scanner utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi selezionati nell'elenco degli archivi. Questa impostazione è attivata di default.

Tutti i tipi di archivio

Se l'opzione è attivata, vengono selezionati e scansionati tutti i tipi di archivi nell'elenco degli archivi.

Archivio estensioni Smart

Se l'opzione è attivata, System Scanner riconosce se un file è in formato compresso (archivio), anche se l'estensione è diversa da quelle abituali, e scansiona l'archivio. Tuttavia a tal fine ogni file deve essere aperto, riducendo così la velocità della scansione. Esempio: se un archivio *.zip ha estensione *.xyz, System Scanner decomprime anche tale archivio e lo scansiona. Questa impostazione è attivata di default.

> **Nota**
> Vengono scansionati solo quei tipi di archivio che sono selezionati nell'elenco degli archivi.

Limita la profondità di ricorsione

La decompressione e la scansione di archivi particolarmente ramificati può necessitare di molto tempo e molte risorse del sistema. Se l'opzione è attivata, è possibile limitare la profondità di ricorsione della scansione in archivi multipli a un determinato numero di livelli di compressione (profondità di ricorsione massima). In questo modo è possibile risparmiare tempo e risorse del processore.

> **Nota**
> Per individuare un virus o un programma indesiderato all'interno di un archivio,

System Scanner deve eseguire la scansione fino al livello di ricorsione nel quale si trova il virus o il programma indesiderato.

Massima profondità di ricorsione

Per poter indicare la profondità massima di ricorsione, l'opzione **Limita la profondità di ricorsione** deve essere attivata.
È possibile inserire direttamente la profondità di ricorsione desiderata oppure modificarla per mezzo dei tasti freccia a destra del campo. I valori consentiti sono compresi tra 1 e 99. Il valore standard e consigliato è 20.

Valori standard

Il pulsante crea i valori predefiniti per la scansione degli archivi.

Elenco archivi

In questa sezione è possibile impostare quali archivi devono essere scansionati da System Scanner. A tal fine è necessario selezionare le voci corrispondenti.

Eccezioni

File che System Scanner deve tralasciare (le opzioni sono disponibili solo se la modalità esperto è attiva)

L'elenco in questa finestra contiene file e percorsi che non devono essere presi in considerazione da System Scanner durante la ricerca di virus e programmi indesiderati.

Si consiglia di inserire quante meno eccezioni possibili e solo i file che non devono essere scansionati durante una scansione normale per qualsivoglia motivo. Consigliamo di far comunque controllare la presenza di virus o programmi indesiderati in questi file prima di inserirli in questo elenco!

Nota
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Questi file non vengono presi in considerazione durante la scansione!

Nota
I file inseriti in questo elenco vengono segnalati nel file di report. Controllare di tanto in tanto nel file di report la presenza di questi file non scansionati poiché potrebbe non sussistere più il motivo per il quale sono stati esclusi. In questo caso i nomi di questi file dovrebbero essere rimossi dall'elenco.

Campo

Inserire in questo campo il nome del file che non deve essere preso in considerazione durante una scansione diretta. Di default non è indicato alcun file.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se si è fornito un nome di file con un percorso completo, tale file non viene scansionato. Se si è inserito un nome di file senza un percorso, ogni file con tale nome (indipendentemente dal percorso o dal drive) non verrà scansionato.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

> **Nota**
> Se si aggiunge un'intera partizione all'elenco dei file da escludere, verranno tralasciati dalla scansione solo i file salvati direttamente nella partizione e non i file contenuti in directory all'interno della partizione:
> Esempio: file da escludere: `D:\` = `D:\file.txt` viene escluso dalla scansione di System Scanner, `D:\folder\file.txt` non viene escluso dalla scansione.

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. Le opzioni sono disponibili solo se la modalità esperto è attiva.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

10.1.2 Report

System Scanner possiede una funzione di log molto ampia. In questo modo si ricevono informazioni esatte sui risultati di una scansione diretta. Il file di report contiene tutte le voci del sistema e gli avvisi e i messaggi della scansione diretta. Le opzioni sono disponibili solo se la modalità esperto è attiva.

> **Nota**
> Per comprendere quali azioni System Scanner ha eseguito in caso di rilevamento di virus o programmi indesiderati, deve sempre essere creato un file di report.

Funzione di log

Disabilitato

Se l'opzione è attivata, System Scanner non riporta le azioni e i risultati della scansione diretta.

Standard

Se l'opzione è attivata, System Scanner riporta il nome dei file infetti con il percorso. Nel file di report vengono riportate inoltre la configurazione per la scansione corrente, le informazioni sulla versione e sul proprietario della licenza.

Esteso

Se l'opzione è attivata, System Scanner riporta anche gli avvisi e le note, oltre alle informazioni standard. un suffisso "(cloud)"

10.2 Real-Time Protection

La rubrica Real-Time Protection della configurazione è dedicata alla configurazione della scansione in tempo reale. Le opzioni sono disponibili solo se la modalità esperto è attiva.

10.2.1 Scansione

Solitamente si desidera che il proprio sistema sia costantemente monitorato. A tal fine utilizzare Real-Time Protection (scansione in tempo reale = On-Access-Scanner). In questo modo è possibile ricercare la presenza di virus e programmi indesiderati in tutti i file che vengono aperti o copiati sul computer, "on the fly". L'opzione è disponibile solo se la modalità esperto è attiva.

File

Real-Time Protection può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione.

> **Nota**
> Se **Tutti i file** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il programma decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza l'elenco delle estensioni**, ma molto più sicura poiché i controlli non vengono effettuati solamente sulla base delle estensioni dei file.

> **Nota**
> Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza l'elenco delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file**". Questa impostazione è attivata di default ed è consigliata.

> **Nota**
> Se questa opzione è attiva e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza l'elenco delle estensioni**". Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o rimuovere voci.

> **Nota**
> Prestare attenzione al fatto che l'elenco estensioni dei file può variare da versione a versione.

Modalità di scansione

Qui si stabilisce il momento in cui effettuare la scansione di un file.

Scansione in lettura

Se l'opzione è attivata, Real-Time Protection scansiona i file prima che vengano letti o eseguiti da un'applicazione o dal sistema operativo.

Scansione in scrittura

Se l'opzione è attivata, Real-Time Protection controlla un file in scrittura. Solo al termine di questa procedura è possibile accedere nuovamente al file.

Scansione in lettura e scrittura

Se l'opzione è attivata, Real-Time Protection scansiona i file prima dell'apertura, della lettura e dell'esecuzione e dopo la scrittura. Questa impostazione è attivata di default ed è consigliata.

Archivi

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Questa opzione è disattivata di default. La scansione degli archivi viene limitata dalla profondità di ricorsione, dal numero di file da scansionare e dalle dimensioni dell'archivio. È possibile impostare la profondità di ricorsione massima, il numero di file da scansionare e le dimensioni massime dell'archivio.

Nota
L'opzione è disattivata di default poiché il processo occupa molta memoria. Generalmente si consiglia di scansionare gli archivi con la scansione diretta.

Massima profondità di ricorsione

Per la ricerca negli archivi, Real-Time Protection utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. L'utente può stabilire la profondità di ricorsione. Il valore standard per la profondità di ricorsione è 1 ed è quello consigliato: tutti i file che si trovano direttamente nell'archivio principale vengono scansionati.

Numero massimo di file

Per la ricerca negli archivi la scansione viene limitata a un numero massimo di file dell'archivio. Il valore standard per il numero massimo di file da scansionare è 10 ed è quello consigliato.

Dimensione massima (KB)

Per la ricerca negli archivi la scansione viene limitata a una dimensione massima degli archivi da decomprimere. Il valore standard è 1000 KB ed è quello consigliato.

Azione in caso di rilevamento

Utilizza log eventi

Se l'opzione è attivata, a ogni rilevamento viene inserita una voce nel log eventi di Windows. È possibile richiamare gli eventi nel visualizzatore eventi di Windows. Questa impostazione è attivata di default. L'opzione è disponibile solo se la modalità esperto è attiva.

Eccezioni

Con queste opzioni è possibile configurare gli oggetti soggetti a eccezioni di Real-Time Protection (scansione in tempo reale). Gli oggetti identificati verranno così esclusi dalla scansione in tempo reale. Real-Time Protection può ignorare gli accessi ai file riportati nell'elenco dei processi da tralasciare durante la scansione in tempo reale. Questa funzione è utile ad esempio per le banche dati o le soluzioni di backup. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Nell'indicare i processi e gli oggetti file da escludere, prestare attenzione a quanto segue: l'elenco viene elaborato dall'alto verso il basso. Più lungo è l'elenco, maggiore è il tempo di cui il processore ha bisogno per elaborare l'elenco a ogni accesso. Si consiglia pertanto di mantenere l'elenco più breve possibile.

Processi che Real-Time Protection deve tralasciare

Tutti gli accessi ai file dei processi indicati in questo elenco vengono ignorati da Real-Time Protection.

Campo

Inserire in questo campo il nome del processo che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun processo.

Il percorso indicato e il nome del file del processo non possono superare i 255 caratteri. È possibile inserire fino a 128 processi. Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Per indicare i processi è possibile utilizzare caratteri Unicode. Pertanto, è possibile indicare nomi di processi o directory che contengono caratteri speciali.

I drive devono essere indicati nel modo seguente: `[lettera del drive]:\`

Il simbolo dei due punti (:) deve essere utilizzato solo per indicare il drive.

Per indicare il processo, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere):

```
C:\Programmi\Applicazioni\applicazione.exe
C:\Programmi\Applicazioni\applicazion?.exe
C:\Programmi\Applicazione\applic*.exe
C:\Programmi\Applicazioni\*.exe
```

Per evitare che l'intero processo venga escluso dal monitoraggio di Real-Time Protection, i dati che contengono esclusivamente i seguenti caratteri non sono validi: * (asterisco), ? (punto interrogativo), / (barra), \ (barra rovesciata), . (punto), : (due punti).

È possibile escludere dal monitoraggio di Real-Time Protection i processi senza percorso completo: `applicazione.exe`

Ciò è valido solo per i processi i cui file eseguibili si trovano sul drive dell'hard disk.

Non indicare alcuna eccezione per i processi i cui file eseguibili si trovano su drive dinamici. I drive dinamici vengono utilizzati per i supporti dati rimovibili, quali CD, DVD o penna USB.

Attenzione
Prestare attenzione al fatto che tutti gli accessi ai file, che vengono avviati da processi e che sono stati evidenziati nell'elenco, sono esclusi dalla scansione di virus e programmi indesiderati!

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare un file eseguibile.

Processi

Il pulsante "**Processi**" apre la finestra "*Selezione del processo*", in cui vengono indicati i processi in corso.

Aggiungi

Con il pulsante è possibile accettare il processo indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si rimuove un processo selezionato dalla finestra di dialogo.

File che Real-Time Protection deve tralasciare

Tutti gli accessi ai file degli oggetti indicati in questo elenco vengono ignorati da Real-Time Protection.

Campo

Inserire in questo campo il nome del file che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun file.

Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Per indicare i file da tralasciare, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere). È possibile anche escludere singole estensioni di file (incluse le wildcard):

```
C:\directory\*.mdb
*.mdb
*.md?
*.xls*
C:\directory\*.log
```

I nomi delle directory devono concludersi con una barra rovesciata \.

Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.

Per ogni drive è possibile indicare al massimo 20 eccezioni con il percorso completo (che inizia con la lettera del drive).

Ad es.: `C:\Programmi\Applicazioni\Nome.log`

Il numero massimo di eccezioni senza percorso completo è 64. Ad es.:

```
*.log
```

In caso di drive dinamici, collegati (montati) come directory a un altro drive, è necessario utilizzare nell'elenco delle eccezioni il nome dell'alias del sistema operativo per il drive collegato:
ad esempio
`\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Anche utilizzando il punto di montaggio stesso (mount point), ad esempio `C:\DynDrive`, si esegue comunque la scansione del drive dinamico. È possibile verificare i nomi dell'alias del sistema operativo dal file di report di Real-Time Protection.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare i file da escludere.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante "Elimina" si rimuove un oggetto file selezionato dalla finestra di visualizzazione.

Per indicare le eccezioni, attenersi alle seguenti indicazioni

Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Un nome di file che contiene wildcard non deve concludersi con una barra rovesciata.
Ad esempio:
`C:\Programmi\Applicazione\applic*.exe`
Questa voce non è valida e non viene considerata come un'eccezione!

In base al file di report di Real-Time Protection è possibile verificare i percorsi utilizzati da Real-Time Protection durante la scansione dei file infetti. Nell'elenco delle eccezioni, utilizzare di massima gli stessi percorsi. Procedere come segue: impostare la funzione di log di Real-Time Protection nella configurazione in Report su **Completo**. Accedere, dopo aver attivato Real-Time Protection, a dati, directory, drive collegati . È possibile leggere il percorso da utilizzare dal file di report di Real-Time Protection. È possibile richiamare il file di report nel Control Center in Real-Time Protection.

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. L'opzione è disponibile solo se la modalità esperto è attiva.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

10.2.2 Report

Real-Time Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento. L'opzione è disponibile solo se la modalità esperto è attiva.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Real-Time Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di log, ad esempio solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Real-Time Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa impostazione è attivata di default.

Esteso

Se l'opzione è attivata, Real-Time Protection riporta nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Real-Time Protection registra tutte le informazioni, anche quelle relative alla dimensione, al tipo di file, alla data ecc., nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata, viene eseguito un backup del file di report prima della limitazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Nota
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

10.3 Aggiornamento

Nella rubrica **Aggiornamento** è possibile configurare l'esecuzione automatica degli aggiornamenti. È possibile impostare diversi intervalli di aggiornamento,.

Aggiornamento automatico

Ogni n giorni/ore/minuti

In questo campo è possibile indicare l'intervallo in cui devono essere eseguiti gli aggiornamenti automatici. Per modificare l'intervallo di aggiornamento, è possibile indicare un dato temporale nel campo e modificarlo mediante i tasti freccia a destra del campo.

Ripeti job se il tempo è scaduto

Se l'opzione è attivata, vengono eseguiti job di aggiornamento scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento. L'opzione è disponibile solo se la modalità esperto è attiva.

10.3.1 Server Web

Server Web

L'aggiornamento può essere eseguito direttamente mediante server Web in Internet . Le opzioni sono disponibili solo se la modalità esperto è attiva.

Connessione al server Web

Utilizza una connessione esistente (rete)

Questa impostazione viene visualizzata se si utilizza la connessione mediante una rete.

Utilizza la seguente connessione

Questa impostazione viene visualizzata se si definisce individualmente la connessione.

L'Updater riconosce automaticamente quali opzioni di connessione sono disponibili. Le opzioni di connessione non disponibili sono grigie e non possono essere attivate. Ad esempio, è possibile stabilire manualmente una connessione dial-up mediante una voce dell'elenco telefonico di Windows.

Utente

Inserire il nome utente dell'account selezionato.

Password

Inserire la password per questo account. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Nota
Se sono stati dimenticati il nome utente o la password di un account Internet, contattare il provider di servizi Internet.

Nota
La selezione automatica dell'Updater mediante i cosiddetti tool dial-up (ad esempio SmartSurfer, Oleco, ...) attualmente non è ancora disponibile.

Termina nuovamente la connessione dial-up aperta per l'aggiornamento

Se l'opzione è attivata, la connessione dial-up aperta per l'aggiornamento viene interrotta automaticamente non appena il download è stato eseguito con successo.

Nota
In Vista e Windows 7 l'opzione non è disponibile. In Vista e Windows 7 la connessione dial-up aperta per l'aggiornamento viene sempre interrotta al termine del download.

Impostazioni proxy

Server proxy

Non utilizzare un server proxy

Se l'opzione è attivata, la connessione al server Web non viene effettuata mediante un server proxy.

Utilizza impostazioni di sistema di Windows

Se l'opzione è attivata, vengono utilizzate le impostazioni di sistema di Windows correnti per la connessione al server Web mediante un server proxy. Per configurare le impostazioni di sistema di Windows in modo tale che venga utilizzato un server proxy, accedere a **Pannello di controllo > Opzioni Internet > Connessioni > Impostazioni LAN**. Per accedere a Opzioni Internet è possibile utilizzare anche il menu **Strumenti** di Internet Explorer.

Attenzione
Se si utilizza un server proxy che richiede l'autenticazione, specificare tutti i dati in**Utilizza questo server proxy**. L'opzione **Utilizza impostazioni di sistema di Windows** può essere selezionata solo in presenza di server proxy che non richiedono alcuna autenticazione.

Utilizza questo server proxy

Se l'opzione è attivata, la connessione al server Web avviene mediante un server proxy, utilizzando le impostazioni definite dall'utente.

Indirizzo

Immettere il nome del computer o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Porta

Inserire il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Nome login

Inserire un nome utente per il login al server proxy.

Password login

Inserire la password appropriata per il login al server proxy. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Esempi:

Indirizzo: `proxy.dominio.it` porta: `8080`

Indirizzo: `192.168.1.100` porta: `3128`

10.4 Web Protection

La rubrica **Web Protection** in **Configurazione > Sicurezza Internet** è dedicata alla configurazione di Web Protection.

10.4.1 Scansione

Web Protection consente la protezione da virus e malware che giungono sul computer attraverso i siti Web caricati da Internet nel browser Web. Nella rubrica **Scansione** è possibile impostare il comportamento di Web Protection. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Scansione

Supporto di IPv6

Se l'opzione è attivata, viene supportata la versione 6 del protocollo Internet di Web Protection.

Protezione Drive-by

La *protezione Drive-by* consente di effettuare impostazioni per bloccare gli iframe, detti anche inline frame. Gli iframe sono elementi HTML, ovvero elementi di siti Internet, che

delimitano un'area di un sito Web. Gli iframe consentono di caricare e visualizzare altri contenuti Web, per lo più di altri URL, come documenti indipendenti in una sottofinestra del browser. Gli iframe vengono principalmente utilizzati per i banner pubblicitari. In alcuni casi gli iframe vengono utilizzati per nascondere virus e malware. In questi casi l'area dell'iframe nel browser è appena o per niente visibile. L'opzione **Blocca iframe sospetti** consente di controllare e di bloccare il caricamento di iframe.

Blocca iframe sospetti

Se l'opzione è attivata, gli iframe dei siti Web richiesti vengono verificati in base a determinati criteri. Se in uno dei siti Web richiesti sono presenti iframe sospetti, l'iframe viene bloccato. Nella finestra dell'iframe viene visualizzato un messaggio d'errore.

Azione in caso di rilevamento

È possibile stabilire delle azioni che Web Protection deve eseguire quando viene rilevato un virus o un programma indesiderato. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Interattivo

Se l'opzione è attivata, durante la scansione diretta in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come procedere con i file infetti. Questa impostazione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, quando un download o lo scaricamento del contenuto di pagine Web supera un timeout di 20 secondi viene visualizzato un messaggio sul desktop con una barra di progressione per il download. Questo messaggio sul desktop è utile in particolare per il controllo del download da pagine Web con grandi volumi di dati: navigando con Web Protection i contenuti delle pagine Web non vengono caricati gradualmente nel browser Internet poiché, prima di essere visualizzati nel browser Internet, vengono scansionati alla ricerca di virus e malware. Questa opzione è disattivata di default.

È possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Web Protection reagisce conformemente alle impostazioni definite in questa sezione.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Web Protection rileva un virus o un programma indesiderato.

Nega accesso

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore

relativo al divieto di accesso. Web Protection inserisce il rilevamento nel file di report, a condizione che la funzione di report sia attivata.

Sposta in quarantena

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inviati in quarantena in caso di rilevamento di un virus o di malware. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo oppure, se necessario, inviato ad Avira Malware Research Center.

Ignora

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inoltrati da Web Protection al proprio browser Web. L'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Accessi bloccati

In **Accessi bloccati** è possibile immettere i tipi di file e i tipi MIME (tipi di contenuto dei dati trasmessi) che devono essere bloccati da Web Protection. Web Protection impedisce il trasferimento dei file da Internet al computer. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Tipi di file / MIME che Web Protection deve bloccare

Tutti i tipi di file e i tipi MIME (tipo di contenuto dei dati trasmessi) nell'elenco vengono bloccati da Web Protection.

Campo

In questo campo immettere i nomi dei tipi MIME e dei tipi di file che devono essere bloccati da Web Protection. Per i tipi di file inserire l'estensione del file, ad es. **.htm**. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio **video/mpeg** o **audio/x-wav**.

> **Nota**
> I file che sono già stati salvati come file Internet temporanei sul computer vengono sicuramente bloccati da Web Protection, ma possono comunque essere caricati dal browser Internet locale dal computer. I file temporanei Internet sono file che vengono memorizzati sul computer dal browser Internet per poter visualizzare le pagine Web più rapidamente.

> **Nota**
> L'elenco dei tipi di file e dei tipi MIME da bloccare viene ignorato per le voci dell'elenco dei tipi di file e dei tipi MIME da tralasciare in Eccezioni.

> **Nota**
> Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Tipi MIME: esempi per tipi di supporto

- `text` = per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `application/octet-stream` = i file del tipo MIME application/octet-stream (eseguibili *.bin, *.exe, *.com, *dll, *.class) vengono bloccati da Web Protection.
- `application/olescript` = i file del tipo MIME application/olescript (file di script ActiveX *.axs) vengono bloccati da Web Protection.
- `.exe` = tutti i file con l'estensione .exe (file eseguibili) vengono bloccati da Web Protection.
- `.msi` = tutti i file con estensione .msi (Windows Installer) vengono bloccati da Web Protection.

Aggiungi

Con il pulsante è possibile accettare il tipo di MIME o di file immesso nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

Eccezioni

Queste opzioni consentono di escludere tipi di MIME (tipi di contenuto dei file trasferiti) e tipi di file per gli URL (indirizzi Internet) dalla scansione di Web Protection. Gli URL e i tipi di MIME indicati vengono ignorati da Web Protection, ovvero durante la trasmissione al computer dell'utente non viene effettuata la scansione di questi dati per verificare la presenza di virus e malware. Le opzioni sono disponibili solo se la modalità esperto è attiva.

Tipi MIME che Web Protection deve tralasciare

In questo campo è possibile selezionare tipi MIME (tipi di contenuto dei dati trasferiti) che devono essere esclusi dalla scansione di Web Protection.

Tipi di file / tipi MIME (personalizzati) che Web Protection deve tralasciare

Tutti i tipi di file e i tipi MIME (tipi di contenuto dei dati trasferiti) nella lista vengono esclusi dalla scansione di Web Protection.

Campo

Inserire in questo campo i nomi dei tipi MIME e i tipi di dati che si intendono escludere dalla scansione di Web Protection. Per i tipi di file inserire l'estensione del file, ad esempio `.htm`. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio `video/mpeg` o `audio/x-wav`.

Nota
Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Attenzione
Tutti i tipi di file e di contenuto nell'elenco delle eccezioni vengono caricati nel browser Internet senza ulteriori verifiche di blocco dell'accesso (elenco dei tipi di file e di MIME da bloccare in Accessi bloccati) o di Web Protection: per tutte le voci dell'elenco delle eccezioni viene ignorato il contenuto dell'elenco dei tipi di file e di MIME da bloccare. Non viene eseguita alcuna scansione per virus e malware.

Tipi MIME: esempi per tipi di supporto

- `text` = per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `audio/` = tutti i file del tipo supporto audio vengono esclusi dalla scansione di Web Protection
- `video/quicktime` = tutti i file video di sottotipo Quicktime (*.qt, *.mov) vengono esclusi dalla scansione di Web Protection
- `.pdf` = tutti i file Adobe-PDF vengono esclusi dalla scansione di Web Protection.

Aggiungi

Con il pulsante è possibile accettare il tipo di MIME o di file immesso nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

URL che Web Protection deve tralasciare

Tutti gli URL di questo elenco vengono esclusi dalla scansione di Web Protection.

Campo

Immettere in questo campo gli URL (indirizzi Internet) che devono essere esclusi dalla scansione di Web Protection, ad esempio **www.domainname.com**. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: .domainname.it per tutte le pagine e tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: **domainname.**. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net).

Nota
Nell'immissione degli URL è possibile utilizzare anche wildcard * per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (valido ma non consigliato)
Le immissioni senza punti quali `*name*` vengono interpretati come parti di dominio di livello superiore e non sono consigliati.

Attenzione
Tutti i siti Web dell'elenco degli URL da escludere vengono caricati nel browser Internet senza ulteriori verifiche : Non viene eseguita alcuna scansione per virus e malware. Si consiglia pertanto di escludere dalla scansione di Web Protection solo URL affidabili.

Aggiungi

Con il pulsante è possibile accettare gli URL (indirizzi Internet) inseriti nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

Esempi: URL da tralasciare

- `www.avira.com` -OPPURE- `www.avira.com/*`
  = tutti gli URL con il dominio www.avira.com vengono esclusi dalla scansione di Web Protection: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html, ...
  Gli URL con dominio www.avira.it vengono esclusi dalla scansione di Web Protection.
- `avira.com` -OPPURE- `*.avira.com`
  = tutti gli URL con dominio di livello secondario o superiore "avira.com" vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini secondari esistenti di "avira.com": www.avira.com, forum.avira.com,...
- `avira.` -OPPURE- `*.avira.*`
  = tutti gli URL con dominio di livello secondario "avira" vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di ".avira.": www.avira.com, www.avira.it, forum.avira.com,...
- `.*domain*.*`
  = tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri "domain" vengono esclusi dalla scansione di Web Protection: www.domain.com, www.new-domain.it, www.sample-domain1.it, ...
- `net` -OPPURE- `*.net`
  = tutti gli URL con dominio di livello superiore "net" vengono esclusi dalla scansione di Web Protection: www.name1.net, www.name2.net, ...

> **Attenzione**
> Indicare tutti gli URL che si desidera escludere dalla scansione di Web Protection in modo più preciso possibile. Evitare l'immissione di tutti i domini di livello superiore o parti di nomi di domini secondari, poiché vi è il rischio che le pagine Internet, che diffondono malware e programmi indesiderati mediante dati globali, vengano escluse dalla scansione di Web Protection come eccezione. Si consiglia di immettere almeno il dominio secondario e il dominio di livello superiore completi: domainname.com

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. Le opzioni sono disponibili solo se la modalità esperto è attiva.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della

protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il prodotto Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

10.4.2 Report

Web Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Web Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di log, ad esempio solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata Web Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, le informazioni meno importanti vengono ignorate per una sintesi migliore. Questa impostazione è attivata di default.

Esteso

Se l'opzione è attivata, Web Protection riporta nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Web Protection registra tutte le informazioni, anche quelle relative alla dimensione, al tipo di file, alla data ecc., nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione fissata di 50 Kilobyte, vengono automaticamente eliminate le voci più vecchie fin quando non si raggiunge una dimensione inferiore del 20%.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

> **Nota**
> Se non sono state specificate limitazioni per i file di report, vengono automaticamente eliminate le voci più vecchie quando il file di report raggiunge le dimensioni di 100 MB. Viene eliminato un numero di voci tali da consentire al file di report di raggiungere una dimensione di 80 MB.

10.5 Protezione dei bambini

Utilizzare le funzioni di Avira *PROTEZIONE DEI BAMBINI* per garantire a bambini o ad altri utenti che utilizzano il computer un'esperienza di navigazione su Internet sicura.

10.6 Protezione mobile

Avira protegge non solo i computer da malware e virus, ma anche i telefoni cellulari e gli smartphone con sistema operativo Android da furto e/o smarrimento. Grazie alla blacklist di Avira Free Android Security, è possibile bloccare le chiamate e gli SMS indesiderati. È sufficiente aggiungere alla blacklist i numeri di telefono da bloccare estrapolandoli dal Registro chiamate, dall'elenco dei messaggi o dall'elenco dei contatti oppure inserendoli manualmente.

10.6.1 Android Security

Avira Free Android Security

Avira Free Android Security presenta due componenti:

- La vera e propria app che viene installata sul dispositivo Android
- La Console Web Android di Avira necessaria alla registrazione e alla gestione delle funzioni

Requisiti di sistema

Sistema operativo:

- Android 2.2 (Froyo)
- Android 2.3.7 (Gingerbread)
- Android 4.0.x (Ice Cream Sandwich)
- Android 4.1.x (Jelly Bean)

Memoria principale

- 1,28 MB di memoria principale libera

Browser:

- Mozilla Firefox
- Google Chrome
- Opera
- Internet Explorer IE7 o superiore

> **Nota**
> Il software Java deve essere installato e attivo, ed è inoltre necessario disporre di una connessione Internet stabile.

Funzionalità

In caso di smarrimento del dispositivo, Avira Free Android Security offre all'utente la possibilità di usufruire di quattro funzioni per la protezione dei dati personali tramite la Console Web Android di Avira:

Allarme da remoto

L'utente attiva sul dispositivo un allarme della durata di 20 secondi.

Individua da remoto

L'utente attiva un comando di posizionamento che individua i parametri di posizionamento del dispositivo.

Blocca da remoto

L'utente può bloccare subito il dispositivo utilizzando un PIN a quattro cifre.

Cancellazione dati da remoto

L'utente può rimuovere i dati memorizzati sulla scheda SIM o su schede di memoria interne ed esterne. Tramite la Console Web è possibile anche ripristinare sul dispositivo le impostazioni predefinite.

> **Nota**
> Per attivare il comando **Ripristino impostazioni predefinite**, da utilizzare per eliminare tutti i dati in caso di smarrimento o furto del dispositivo, durante l'installazione è necessario attivare l'opzione **Amministratore dispositivo**.

La funzione Blacklist di Avira Free Android Security consente di bloccare le chiamate e gli SMS indesiderati.

Blacklist

Per aggiungere i contatti indesiderati alla blacklist, è possibile estrapolarli dal Registro chiamate, dall'elenco dei messaggi o dall'elenco dei contatti oppure inserirli manualmente.

La Console Web

La Console Web Avira è un'applicazione basata su browser da utilizzare per la gestione delle funzioni di protezione. Nella Dashboard della Console Web è possibile gestire il proprio account e attivare le funzioni da remoto, quali **Individua**, **Blocca**, **Attiva allarme** o **Elimina**.

La Console Web Avira si compone di una barra del titolo, una barra laterale e una schermata principale con più schede. Nella barra del titolo sono riportati i dati di accesso dell'utente e i link per accedere all'area Supporto e alla gestione dell'account. Nella barra

laterale sono elencati i dispositivi registrati. Nella schermata principale della Console Web sono disponibili tutte le funzioni di protezione dell'app nonché informazioni sulla funzione **Blacklist** attivata sul dispositivo.

Barra del titolo della console Web

Dettagli account

Nella barra del titolo sono visualizzati i link **Supporto** Avira, **Account** utente, **Esci** e i dati di accesso dell'utente.

- Fare clic sul link **Account**.
  - ↳ Verrà visualizzata la finestra **Dettagli account**, contenente i seguenti campi:

Data di creazione

Indica la data e l'ora in cui l'utente ha creato l'account.

Nome

Qui l'utente può inserire il proprio nome di battesimo.

Cognome

Qui l'utente può inserire il proprio cognome.

Lingua

Selezionare la lingua desiderata nel menu a discesa.

Paese

Selezionare un Paese nel menu a discesa.

Tipo di account

Indica il tipo di account utilizzato dall'utente.

Salva modifiche

- Fare clic su **Salva modifiche** per salvare le modifiche apportate ai dati dell'account.

Gestione password

Nella barra del titolo della Console Web Avira è disponibile il link **Account**, in cui l'utente può anche gestire la propria password.

- Fare clic sul link **Account**.
  - ↳ Verrà visualizzata la finestra **Gestione password**, contenente i seguenti campi:

Password

Immettere una nuova password per l'account Avira Free Android Security.

Conferma password

Inserire nuovamente la password per conferma.

Modifica password

- Fare clic sul pulsante per salvare le modifiche apportate.

Protezione dell'account

Nella barra del titolo della Console Web Avira è disponibile il link **Account**, in cui l'utente può anche impostare una domanda di sicurezza. La domanda di sicurezza è funzionale a una maggiore protezione dell'account. Se l'utente dimentica i dati di accesso oppure desidera modificare l'indirizzo e-mail, può eseguire l'autenticazione con l'ausilio della domanda di sicurezza.

- Fare clic sul link **Account**.
  - ↳ Verrà visualizzata la finestra **Protezione dell'account**, contenente i seguenti campi:

Domanda di sicurezza

Consente di accedere al menu a discesa in cui sono elencate le domande di sicurezza. Selezionarne una a cui solo l'utente è in grado di rispondere correttamente.

Risposta

- Inserire la risposta in questo campo.
- Assicurarsi che la risposta non contenga alcun errore ortografico e possa essere ricordata facilmente.

Salva modifiche

- Fare clic su Salva modifiche per salvare la domanda di sicurezza e la relativa risposta.

Gestione dispositivi

Nella barra del titolo della Console Web Avira è disponibile il link **Account**, in cui l'utente può anche gestire i propri dispositivi.

- ↳ Fare clic sul link **Account**.
- ↳ Verrà visualizzata la finestra **Gestione dispositivi**, contenente i seguenti campi:

Dispositivi disponibili

Consente di accedere al menu a discesa e selezionare un dispositivo.

Elimina dispositivo

- Fare clic sul pulsante per eliminare dall'account il dispositivo selezionato.

Come procedere

In che modo è possibile modificare l'indirizzo e-mail?

Se si desidera modificare l'indirizzo e-mail, rivolgersi al Supporto Avira. L'indirizzo e-mail viene utilizzato non solo come informazione di contatto dell'utente, ma anche come ID utente. Di conseguenza, non è possibile modificare l'indirizzo e-mail autonomamente tramite la Console Web o un'app del dispositivo.

In che modo è possibile proteggere i dati salvati sul dispositivo?

La soluzione più semplice e rapida per proteggere i dati salvati sul dispositivo consiste nel bloccare il dispositivo stesso.

- Effettuare il login alla Console Web.
- Accedere alla scheda **Blocca**.
- Immettere un PIN a quattro cifre.
- Confermare il PIN.
- Fare clic su **Blocca**.
  - ↳ A questo punto, il PIN potrà essere utilizzato per bloccare e sbloccare il dispositivo.

> **Nota**
> La validità del PIN è solo temporanea. Per ogni blocco/sblocco del dispositivo è necessario immettere un nuovo PIN.

Se il PIN è stato dimenticato oppure per tre volte è stato inserito un PIN errato, in che modo è possibile sbloccare il dispositivo?

In questo caso è necessario accedere alla Console Web e modificare il PIN.

- Effettuare il login alla Console Web.
- Accedere alla scheda **Blocca**.
- Immettere un PIN a quattro cifre.
- Confermare il PIN.
- Fare clic su **Blocca**.
  - ↳ A questo punto, il PIN potrà essere utilizzato per bloccare e sbloccare il dispositivo.

In che modo è possibile modificare il PIN?

Per modificare il PIN è necessario accedere alla Console Web. Non è consentito modificare il PIN tramite l'app stessa.

- Effettuare il login alla Console Web.
- Accedere alla scheda **Blocca**.
- Immettere un PIN a quattro cifre.
- Confermare il PIN.
- Fare clic su **Blocca**.
  - ↳ A questo punto, il PIN potrà essere utilizzato per bloccare e sbloccare il dispositivo.

In che modo è possibile rintracciare il dispositivo in caso di smarrimento o furto?

In caso di smarrimento o furto del dispositivo, Avira Free Android Security offre all'utente le seguenti due opzioni per recuperarlo.

Attivazione di un allarme

La funzione **Attiva allarme** semplifica la ricerca del dispositivo. Si rivela particolarmente utile nei casi in cui l'utente ha lasciato il dispositivo nelle immediate vicinanze, ad esempio nella propria abitazione.

- Effettuare il login alla Console Web.
- Selezionare la scheda **Allarme** e fare clic su **Attiva allarme**.
  - ↳ Il dispositivo emetterà quindi un suono ad alto volume per 20 secondi in modo tale da poter essere rintracciato più facilmente. Durante i 20 secondi, l'allarme non può essere disattivato né interrotto. L'allarme viene emesso anche se sul dispositivo è stato disattivato l'audio.

> **Nota**
> Si ricorda, tuttavia, che se il dispositivo è spento oppure la batteria è scarica, l'allarme non verrà emesso.

Ricerca del dispositivo

Se l'utente non sa dove ha smarrito il dispositivo oppure ha motivo di credere che il dispositivo sia stato sottratto, può localizzarne la posizione.

> **Nota**
> La definizione della posizione richiede fino a 3 minuti. In fase di localizzazione del dispositivo, non è possibile riattivare il comando **Individua**. L'attivazione del

comando **Individua** è consentita, tuttavia, per gli altri dispositivi registrati nell'account dell'utente.

- Effettuare il login alla Console Web.
- Selezionare la scheda **Individua**.
  - ↳ Nella Console Web Avira viene visualizzata una sezione tratta da Google Maps.
- Fare clic su **Individua** al di sotto della mappa geografica.
  - ↳ Durante la definizione della posizione viene visualizzato il tempo trascorso. Sulla mappa appare la posizione esatta del dispositivo. Le informazioni geofisiche indicate sono il grado di latitudine e longitudine.

In che modo è possibile registrare un nuovo dispositivo?

Nell'account utente è possibile aggiungere fino a un massimo di 5 dispositivi. Tutti i dispositivi aggiunti tramite l'app a uno stesso account Google o a uno stesso indirizzo e-mail risultano registrati allo stesso account Avira Free Android Security, il che significa che a ogni account e-mail può essere associato un unico account Avira Free Android Security comprendente un massimo di 5 dispositivi.

- Utilizzare il dispositivo che si desidera aggiungere al proprio account per effettuare il download di Avira Free Android Security.
- Installare l'app sul dispositivo.
- Selezionare il proprio account Google o inserire un altro indirizzo e-mail e toccare **Accetta EULA e continua**.
  - ↳ L'utente riceverà all'indirizzo indicato un'e-mail in cui viene confermata la registrazione del nuovo dispositivo all'account Avira Free Android Security esistente.
  - ↳ Accedendo alla Console Web, l'utente potrà quindi visualizzare il nuovo dispositivo nella sezione **Tutti i dispositivi**, sul lato sinistro della Console Web.
- A questo punto, fare clic su **Modifica** all'interno della scheda "Dispositivo" per definire le impostazioni di modifica del nome e del numero di telefono relativi al dispositivo.

Nota
Dal momento che a ogni account Avira Free Android Security possono essere associati soltanto 5 dispositivi, prima di poterne aggiungere un altro è necessario eliminare l'app da un dispositivo registrato. In alternativa, accedere alle impostazioni dell'**account** nella Console Web, selezionare un dispositivo dall'elenco a discesa in **Gestione dispositivi** e fare clic su **Elimina dispositivo**.

Risoluzione dei problemi

Risoluzione dei problemi

Messaggi di errore

Messaggi	Significato
Per continuare, connettersi a una rete mobile o Wi-Fi.	In fase di registrazione non è stata rilevata alcuna connessione di rete. Per continuare, è necessario attivare una connessione di rete.
Il servizio non è attualmente disponibile. Riprovare più tardi.	Il servizio di Google non è disponibile al momento.
Arresto anomalo di Avira Free Android Security! Toccare qui per aiutarci a risolvere il problema.	Si è verificato un errore imprevisto che causerà l'arresto dell'applicazione. Toccare lo schermo per inviarci automaticamente il registro degli errori.
Per registrare il dispositivo è necessario un account Google. Crearne uno e riprovare.	Sul dispositivo non è stato rilevato alcun account Google.
La password dell'account Google è stata modificata. Per aggiornare la password sul dispositivo, aprire Gmail o l'app Google Play.	La password dell'account Google predefinito sul dispositivo non è valida. Verificare se la password di autenticazione per l'account Google è stata modificata. Aggiornare e sincronizzare la password del dispositivo accedendo all'app di Gmail o di Google Play.
Troppe applicazioni sul dispositivo stanno utilizzando il servizio push di Google (GCM). Disinstallarne una e riprovare.	Google stabilisce un limite massimo di applicazioni con servizio GCM installabili su ogni dispositivo.

Si è verificato un errore. Riprovare più tardi.	Si è verificato un errore sconosciuto.
In questo account sono registrati più di cinque dispositivi. Eliminare un dispositivo per poterne aggiungere un altro.	È stato raggiunto il numero massimo di cinque dispositivi registrati in Avira Free Android Security.
Questo dispositivo non è più registrato con un account Avira Free Android Security. L'app è stata quindi ripristinata.	La registrazione è stata annullata poiché il dispositivo in uso è stato eliminato dall'elenco dei dispositivi registrati.
Si è verificato un errore del server. Riprovare più tardi.	Si è verificato un errore del server sconosciuto.
Si è verificato un errore imprevisto che causerà l'arresto dell'applicazione. Aiutateci a risolvere questo problema. È sufficiente fare clic su "OK" per inviarci automaticamente il registro degli errori. Di seguito è inoltre possibile aggiungere commenti su questo problema:	L'applicazione è stata chiusa a causa di un errore imprevisto. Per consentire ad Avira di risolvere il problema, fare clic su OK. In questo modo il registro degli errori verrà inviato automaticamente ad Avira.
Errore imprevisto. Consultare la barra di notifica.	Si è verificato un errore imprevisto.
Grazie!	Grazie per aver segnalato il problema, le informazioni sono state inviate correttamente.
In caso di smarrimento o furto del dispositivo, Avira Free Android Security può aiutare l'utente a eseguire un ripristino delle impostazioni predefinite per cancellare i dati dal dispositivo. Per eseguire un ripristino delle impostazioni predefinite, è necessario attivare l'amministrazione dispositivo.	In caso di smarrimento del dispositivo è possibile utilizzare Avira Free Android Security per eliminare i dati salvati sul dispositivo ripristinando le impostazioni predefinite. A tal fine, è necessario che la funzione **Amministratore dispositivo** sia attiva.

Per continuare, connettersi a una rete mobile o Wi-Fi.	Attivare una connessione di rete per continuare.
Cancellazione dei dati tramite ripristino delle impostazioni predefinite abilitata/disabilitata.	La funzione di cancellazione dei dati tramite il comando **Ripristino impostazioni predefinite** è stata attivata/disattivata.
Dispositivo registrato correttamente in Avira Free Android Security.	Corretta registrazione di Avira Free Android Security.
Un messaggio di posta elettronica è stato inviato a <mario.rossi@gmail.com>. Accedere al proprio account di posta elettronica per leggere le informazioni e le ulteriori indicazioni fornite.	All'indirizzo <mario.rossi@gmail.com> è stato inviato un messaggio di posta elettronica con le informazioni di attivazione. Leggerlo per iniziare a utilizzare il software.
Per eventuali domande in proposito, rivolgersi al forum di supporto o ai dipendenti di Avira.	In caso di domande in proposito, rivolgersi al forum o ai dipendenti di Avira.
Registrazione non riuscita. Riavviare l'app e riprovare.	In fase di registrazione si è verificato un errore imprevisto. Riavviare l'applicazione e ripetere la procedura di registrazione.

Registrazione non riuscita. È possibile che l'utente si avvalga di una tecnologia non compatibile con Avira Free Android Security. Riavviare l'app e riprovare.	Probabilmente sul dispositivo è impiegata una tecnologia non compatibile con Avira Free Android Security. Verificare i requisiti di sistema riportati di seguito. Sistema operativo: Android 2.2 (Froyo) - Android 4.1. (Jelly Bean). Memoria principale: 1,28 MB di memoria principale libera. Browser: Mozilla Firefox, Google Chrome, Opera e Internet Explorer IE7 o superiore.
Creazione contatto non riuscita	Non è stato possibile aggiungere il contatto alla blacklist perché è già presente nell'elenco.
Il nome esiste già nella blacklist.	Il nome indicato è già presente nella blacklist e non può pertanto essere inserito una seconda volta.
Il contatto esiste già nella blacklist.	Il contatto indicato è già presente nella blacklist e non può pertanto essere inserito una seconda volta.
Il numero esiste già nella blacklist alla voce <Mario Rossi>.	Il numero di telefono indicato è già presente nella blacklist alla voce <Mario Rossi> e non può pertanto essere inserito una seconda volta.

Glossario

Abbreviazione	Significato
GCM	Il servizio Android Google Cloud Messaging (GCM) supporta l'invio dei dati presenti sui server alle applicazioni installate sul dispositivo.

IMEI	L'International Mobile Equipment Identity (IMEI) è un codice numerico univoco, paragonabile a un'impronta digitale, che consente l'identificazione dei dispositivi.
Scheda SIM	Il modulo d'identità dell'abbonato (Subscriber Identification Module, SIM) è una scheda su cui sono memorizzate varie informazioni, tra cui ad esempio il numero di serie, il numero di telefono o il PIN.
PIN	Numero di identificazione personale (Personal Identification Number), spesso un codice numerico a quattro cifre.
SO	Sistema operativo installato sul dispositivo.
GPS	Il Global Positioning System è un sistema satellitare in grado di fornire ai ricevitori GPS informazioni sulle coordinate geografiche e sugli orari.
Tecnologia di rete cellulare	Radiotecnica avanzata che consente la ricezione del segnale da parte dei telefoni cellulari e la trasmissione ad altre celle radio mediante onde radio.
Wi-Fi	Standard che consente lo scambio di dati e l'accesso wireless a Internet.
WLAN	Accesso wireless alla rete.
Cloud	Tecnologia informatica che si avvale di server remoti e infrastrutture IT. I dati salvati nel cloud non sono salvati sul computer locale.

Numero di telefono alternativo	Numero di telefono che può essere selezionato dal dispositivo bloccato tramite il pulsante **Chiama proprietario**.
Grado di latitudine	Coordinata geografica che indica la posizione nord-sud sulla Terra.
Grado di longitudine	Coordinata geografica che indica la posizione est-ovest sulla Terra.

Assistenza clienti

Supporto

Assistenza clienti

Sul sito Web http://www.avira.com sono disponibili tutte le informazioni necessarie sul servizio di assistenza clienti.

Community Forum

Prima di contattare la hotline, si consiglia di visitare il forum degli utenti all'indirizzo http://forum.avira.com.
È possibile che il problema dell'utente sia già stato affrontato e risolto all'interno della Community.

FAQ

Leggere anche la sezione "FAQ" disponibile sul sito Web http://www.avira.com/it/support-for-home-knowledgebase
È possibile che la domanda dell'utente sia stata già posta e risolta da altri utenti.

Contatti

Indirizzo

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Germania

Internet

Per ulteriori informazioni sulla nostra azienda e sui nostri prodotti, consultare http://www.avira.com

Funzionamento

La Console Web

Una volta terminata l'installazione, per poter accedere alla Console Web l'utente dovrà registrare il dispositivo.

- La Console Web Avira si compone di una barra del titolo, una barra laterale e una schermata principale con più schede.
- Nella barra del titolo sono riportati i dati di accesso dell'utente e i link per accedere all'area Supporto e alla gestione dell'account. Qui è possibile definire le impostazioni lingua per la Console Web Avira.
- Nella barra laterale sono elencati i dispositivi registrati.
- Ogni dispositivo viene visualizzato singolarmente in un campo separato:
  - Nella scheda del dispositivo fare clic sul pulsante **Modifica** per aprire la scheda **Impostazioni** della Console Web: da qui è possibile gestire il nome e il numero di telefono del dispositivo.
- Nell'area inferiore della barra laterale è disponibile un link tramite il quale l'utente può inserire e salvare una domanda di sicurezza personale.
- Nella schermata principale della Console Web sono disponibili tutte le funzioni di protezione utili al monitoraggio del dispositivo Android nonché informazioni sul contenuto della blacklist.

Le schede della Console Web

Nella Console Web sono presenti le schede riportate di seguito.

- Dashboard
- Individua
- Cancellazione dati
- Allarme
- Blocca
- Blacklist
- Impostazioni

La Dashboard della Console Web di Avira Free Android Security

Nella scheda **Dashboard** sono contenute diverse informazioni sul dispositivo in uso nonché pulsanti di controllo per l'attivazione di operazioni necessarie alla protezione del dispositivo.

Informazioni sul dispositivo

- Marca: marca del dispositivo.
- Modello: denominazione del modello del dispositivo.
- IMEI: l'International Mobile Equipment Identity (IMEI) è un codice numerico univoco composto da 15 cifre che consente l'identificazione dei telefoni cellulari e anche di alcuni telefoni satellitari.
- Versione SO: numero di versione del sistema operativo Android.
- Versione app: numero di versione dell'app Avira in uso. In caso di utilizzo di una versione obsoleta, viene visualizzata un'icona di avviso rossa.
- Gestione disp.: indica se la gestione dei dispositivi è attiva o meno. Se non è attiva, viene visualizzata un'icona di avviso rossa.
- Batteria: informazioni sul livello di carica della batteria espresso in percentuale.
- Numero di telefono: numero di telefono memorizzato sulla scheda SIM.
- Rete: rete cellulare a cui appartiene la scheda SIM.
- Paese: Paese di origine della scheda SIM.
- **Aggiorna**: il pulsante "Aggiorna" consente l'aggiornamento delle informazioni sul dispositivo.

Individua da remoto

- Ultima ricerca: ora in cui è avvenuta l'ultima ricerca del dispositivo, ad esempio "5 ore fa“, "3 giorni fa".
- Grado di latitudine: l'esatta latitudine in cui il dispositivo si trova.
- Grado di longitudine: l'esatta longitudine in cui il dispositivo si trova.

Blocca dispositivo

- Ultima operazione: l'ultima operazione effettuata tramite la Console Web, ad esempio "Blocca".
- Ultima attivazione: ora in cui è avvenuto l'ultimo blocco o sblocco di un dispositivo.

Attiva allarme

- Ultima attivazione: intervallo di tempo trascorso dall'ultimo invio di un allarme al dispositivo.

Elimina dati

- Ultima eliminazione: intervallo di tempo trascorso dall'ultima eliminazione effettuata sul dispositivo.
- Tipo: tipo di eliminazione effettuata sul dispositivo.

Blacklist

- Utilizzare questa funzione per bloccare chiamate e SMS indesiderati.

Individua

Nella scheda **Individua** viene visualizzata una sezione tratta da Google Maps. Al di sotto della mappa geografica viene indicato lo stato di definizione della posizione.

- Fare clic sul pulsante **Individua** per avviare la definizione della posizione del dispositivo smarrito.
  - ↳ La definizione della posizione può richiedere diversi minuti a seconda delle prestazioni di rete e della potenza del segnale.

  Avira Free Android Security ricerca il dispositivo con l'ausilio del sistema GPS, della tecnologia di rete cellulare e della WLAN.

  Durante la definizione della posizione viene visualizzato il tempo trascorso.
  - ↳ Sulla mappa appare la posizione esatta del dispositivo smarrito. Le dimensioni della mappa possono essere ingrandite o ridotte.

Cancellazione dati

> **Nota**
> Se la versione di Avira Free Android Security in uso non supporta la funzione di cancellazione dei dati, eseguire l'aggiornamento dell'app sul dispositivo seguendo le indicazioni fornite nella nostra Knowledge base. In seguito sarà sufficiente aggiornare questa pagina per usufruire appieno della **funzione di cancellazione dei dati**.

Nella scheda **Cancellazione dati** sono disponibili tre opzioni per la cancellazione dei dati dal dispositivo. È possibile anche selezionare più opzioni contemporaneamente. La funzione di cancellazione dei dati comporta una cancellazione definitiva, il che significa che i dati eliminati con tale funzione non possono più essere ripristinati.

> **Nota**
> Prima di attivare la funzione di cancellazione dei dati, è necessario bloccare il dispositivo. Si consiglia vivamente, inoltre, di eseguire prima un backup dei dati importanti.

Scheda SIM

Se si attiva la funzione di cancellazione dei dati per **Scheda SIM**, vengono eliminati tutti i dati presenti nella scheda SIM. Tutti i dati di contatto e gli SMS salvati sulla scheda SIM vengono rimossi. Tali dati non possono più essere ripristinati. Al contrario, i dati salvati sul dispositivo o sulla scheda SD non sono interessati dalla cancellazione.

> **Nota**
> A seconda del tipo di scheda, è possibile che la cancellazione dei dati della scheda SIM non sia consentita.

- Fare clic su **Scheda SIM** per eliminare tutti i dati salvati sulla scheda SIM.
- Confermare la cancellazione facendo clic su **OK**.
  - ↪ Verrà visualizzato il messaggio **Cancellazione dati scheda SIM eseguita correttamente.**
- Fare clic su **OK** per chiudere il messaggio e tornare alla scheda Cancellazione dati.

Intero archivio

Se si attiva la funzione di cancellazione dei dati per **Intero archivio**, vengono eliminati tutti i dati salvati sul dispositivo o sulla scheda SD. Tali dati non possono più essere ripristinati. Al contrario, i dati salvati sulla scheda SIM non sono interessati dall'opzione **Intero archivio**.

- Fare clic su **Elimina archivio** per avviare l'eliminazione dei dati salvati direttamente sul dispositivo o sulla scheda SD.
- Confermare la cancellazione facendo clic su **OK**.
  - ↪ Verrà visualizzato il messaggio **Cancellazione dati archivio eseguita correttamente.**
- Fare clic su **OK** per chiudere il messaggio e tornare alla scheda Cancellazione dati.

Ripristino impostazioni predefinite

Selezionando l'opzione **Ripristino impostazioni predefinite**, vengono ripristinate le impostazioni di fabbrica del dispositivo e, di conseguenza, vengono eliminati tutti gli account, le applicazioni e i dati relativi alle applicazioni salvati sul dispositivo. I dati salvati sulla scheda SIM o sulla scheda SD non sono interessati dalla cancellazione dati effettuata con **Ripristino impostazioni predefinite**.

> **Nota**
> Per attivare il comando **Ripristino impostazioni predefinite**, da utilizzare per eliminare tutti i dati in caso di smarrimento o furto del dispositivo, durante l'installazione è necessario attivare l'opzione **Amministratore dispositivo**.

- Fare clic su **Ripristino impostazioni predefinite** per ripristinare le impostazioni di fabbrica del dispositivo.
- Confermare il tipo di cancellazione dati selezionato facendo clic su **OK**.
- Fare di nuovo clic su **OK** per continuare.

- Per chiudere il messaggio di conferma dell'avvenuto **ripristino delle impostazioni predefinite**, fare clic su **OK**.

> **Attenzione**
> Se si seleziona l'opzione **Ripristino impostazioni predefinite**, viene disinstallata anche l'app Avira Free Android Security. Di conseguenza, non sarà più possibile inviare comandi al dispositivo tramite la Console Web, il che significa che non sarà più possibile bloccare né individuare il dispositivo.

Cancellazione dati combinata

L'opzione **Cancellazione dati combinata** consente di attivare uno, due o tutti e tre i tipi di cancellazione dei dati.

- Selezionare i tipi di cancellazione che si desidera attivare oppure fare clic su **Seleziona tutto** per attivare tutte e tre le opzioni contemporaneamente.
- Fare clic su **Esegui azioni di eliminazione selezionate**.
- Confermare con **OK**.
  - ↳ A seconda delle opzioni selezionate e delle dimensioni dell'archivio del dispositivo, l'azione di eliminazione può richiedere fino a 60 minuti.
- Fare clic su **OK** per continuare.
- Per chiudere il messaggio di conferma dell'avvenuta **cancellazione dati combinata**, fare clic su **OK**.

Qui di seguito vengono riportati i risultati dei tre tipi di cancellazione dei dati.

Opzione di cancellazione dati	Scheda SIM	Intero archivio	Ripristino impostazioni predefinite
SMS sul dispositivo			Eliminati
SMS sulla scheda SIM	Eliminati		
Dati di contatto sul dispositivo			Eliminati
Dati di contatto sulla scheda SIM	Eliminati		

Dati sulla scheda SD		Eliminati	
Dati nell'archivio USB interno		Eliminati	
Account, applicazioni, dati relativi alle applicazioni			Eliminati

Allarme

Dalla scheda **Allarme** è possibile attivare un allarme ad alto volume che verrà emesso dal dispositivo. Questa funzione permette all'utente di trovare subito il proprio dispositivo.

- Fare clic sul pulsante **Attiva allarme** per attivare la funzione di allarme.
  - ↳ Il dispositivo emetterà quindi un suono ad alto volume per 20 secondi. In questo intervallo di tempo, l'allarme non può essere disattivato né interrotto.

La scheda Blocca

Nella scheda **Blocca** è possibile immettere un PIN a quattro cifre utile per bloccare e sbloccare il dispositivo. Qui l'utente può anche inserire un messaggio che verrà visualizzato sullo schermo blocco del dispositivo. All'interno della scheda, inoltre, è possibile aggiungere un numero di telefono che, anche in caso di dispositivo bloccato, potrà essere selezionato con l'ausilio del pulsante **Chiama proprietario**.

> **Nota**
> Per avviare la procedura di cancellazione dei dati, è necessario che il dispositivo sia bloccato. Si consiglia inoltra di bloccare il dispositivo per ragioni di privacy.

- Inserire nel campo **Inserisci PIN** un PIN a quattro cifre.
- Confermare il PIN nel campo sottostante.
  - ↳ È possibile sbloccare il dispositivo manualmente solo se in precedenza è stato inserito un PIN. Se si dimentica il PIN inserito, è necessario sbloccare il dispositivo tramite la Console Web.
- Inserire nel campo **Messaggio per smarrimento dispositivo** un messaggio che verrà visualizzato sul dispositivo in caso di smarrimento. Ad esempio, è possibile

inserire un messaggio e aggiungere il proprio indirizzo e-mail per consentire a chi ritrova il dispositivo di contattare subito l'utente.

- Inserire nel campo **Numero di telefono alternativo** un numero di telefono che potrà essere selezionato dal dispositivo bloccato tramite il pulsante **Chiama proprietario**. Scegliere un numero di telefono sicuro, ad esempio il proprio numero di casa oppure il numero di telefono di un amico.
- Fare clic su **Blocca** per salvare il PIN sul dispositivo e bloccare il dispositivo stesso.
- Fare clic su **Sblocca** se si desidera sbloccare il dispositivo tramite Console Web.

Blacklist

Se l'utente non desidera essere disturbato da determinati SMS o chiamate, ha la possibilità di inserire i relativi numeri di telefono nella blacklist. Questa funzione consente di bloccare le chiamate e gli SMS indesiderati. I numeri di telefono da aggiungere alla blacklist possono essere estrapolati dall'elenco dei contatti, dal Registro chiamate e dai messaggi oppure possono essere inseriti manualmente.

Inserimento nella blacklist di numeri di telefono estrapolati dai registri dei dispositivi

Qui di seguito viene illustrato come aggiungere alla blacklist i numeri presenti nei registri delle chiamate e dei messaggi oppure nell'elenco dei contatti.

- Accedere ad Avira Free Android Security dal dispositivo.
- Toccare **Blacklist**.
  - ↳ Sullo schermo viene visualizzata la **Blacklist**.
- Toccare il pulsante **Aggiungi**.
  - ↳ Sullo schermo viene visualizzato **Aggiungi contatti alla blacklist**.
- Selezionare il registro da cui si desidera estrapolare il numero di telefono da aggiungere alla blacklist e toccare il campo corrispondente.

  Se non si desidera inserire alcun numero di telefono nella blacklist, toccare **Annulla**.

  Toccare il numero di telefono da bloccare.
  - ↳ Sullo schermo verrà quindi visualizzato il numero di telefono e il nome del contatto che si desidera bloccare.
- Selezionare il tipo di contatto che si desidera bloccare. L'utente ha la possibilità di scegliere tra **Chiamate e SMS**, soltanto **Chiamate** oppure soltanto **SMS**.
- Fare clic su **Salva** per salvare il numero di telefono nella blacklist.
- Il numero bloccato viene visualizzato in **Blacklist**.

Nota
Se il contatto da aggiungere è già presente nella blacklist, l'utente riceverà un messaggio di errore.

Inserimento manuale dei numeri di telefono nella blacklist

È possibile inserire i numeri di telefono anche digitandoli all'interno della blacklist.

- Accedere ad Avira Free Android Security dal dispositivo.
- Toccare **Blacklist**.
  - ↳ Sullo schermo viene visualizzata la **Blacklist**.
- Toccare il pulsante **Aggiungi**.
  - ↳ Sullo schermo viene visualizzato **Aggiungi contatti alla blacklist**.
- Se si desidera digitare un numero di telefono, toccare **Crea contatto manualmente**.
  - ↳ Sullo schermo verrà visualizzato **Inserisci dettagli di contatto**.
- Toccare il campo **Nome** per accedere alla tastiera di immissione delle lettere.
- Toccare il campo **Numero di telefono** per accedere alla tastiera di immissione dei numeri.
- Selezionare il tipo di contatto che si desidera bloccare. L'utente ha la possibilità di scegliere tra **Chiamate e SMS**, soltanto **Chiamate** oppure soltanto **SMS**.
- Fare clic su **Salva** per salvare il numero di telefono nella blacklist.

Modifica della blacklist

È possibile modificare il numero di telefono e il nome del contatto bloccato.

- Accedere ad Avira Free Android Security dal dispositivo.
- Toccare **Blacklist**.
  - ↳ Sullo schermo viene visualizzata la **Blacklist**.
- Toccare il contatto da modificare.
  - ↳ Sullo schermo verrà visualizzato **Inserisci dettagli di contatto**.
- Toccare il campo **Nome** per accedere alla tastiera in cui modificare il nome.
- Toccare il campo **Numero di telefono** per accedere alla tastiera in cui modificare il numero.
- Fare clic su **Salva** per salvare nella blacklist le modifiche apportate al contatto.
- Fare clic su **Annulla** nel caso in cui non si desidera salvare le modifiche effettuate.

Eventi bloccati

L'utente può controllare la cronologia di tutti i contatti bloccati accedendo alla scheda **Eventi bloccati**. L'elenco può essere consultato in ordine cronologico oppure per tipo di contatto, ad esempio chiamate o SMS. Vengono visualizzati il nome del contatto, la data, l'ora e le modalità del tentativo di contatto.

- Toccare il pulsante **Tutti** per scegliere l'opzione desiderata tra **Tutti**, **Oggi** e **Nuovo**.
- Toccare il pulsante **Chiamate e SMS** per visualizzare le chiamate e i messaggi bloccati. Selezionare l'opzione **Chiamate** per controllare quale contatto della blacklist ha tentato di effettuare una chiamata verso il numero dell'utente; selezionare invece **SMS** per richiamare i messaggi di testo bloccati.

Eliminazione delle voci presenti in Eventi bloccati

L'utente può eliminare le voci presenti in **Eventi bloccati**. Ordinare l'elenco degli eventi secondo il criterio **Tutti**, **Oggi** o **Nuovo,** e selezionare una tra le opzioni **Chiamate e SMS**, **Chiamate** o soltanto **SMS**. È possibile eliminare gli eventi singolarmente o tutti allo stesso tempo. Se ad esempio si impostano i filtri **Tutti** e **Chiamate**, vengono elencate tutte le chiamate bloccate. L'utente ha quindi la possibilità di eliminare contemporaneamente tutte le chiamate bloccate oppure di selezionare i singoli contatti ed eliminare quindi le chiamate visualizzate.

- Toccare il contatto per il quale si desidera eliminare gli eventi bloccati.
  - ↳ Vengono visualizzati l'ora e il numero delle chiamate e/o degli SMS in entrata.
- Toccare il campo **SMS** per visualizzare il contenuto degli SMS bloccati.
  - ↳ L'utente potrà quindi aprire e leggere i messaggi di testo.
  - ↳ Gli SMS possono essere eliminati singolarmente o tutti allo stesso tempo.

  Toccare **Seleziona tutto** per selezionare tutti gli SMS da eliminare o apporre un segno di spunta accanto ai singoli SMS.

  Toccare **Elimina** per rimuovere questi messaggi di testo oppure toccare **Indietro** per arrestare il processo di eliminazione.

  - ↳ All'utente viene richiesto di confermare l'eliminazione degli SMS bloccati.

  Toccare **Elimina** per eliminare dalla cronologia gli SMS selezionati.

  Toccare **Annulla** per arrestare il processo di eliminazione.
- Toccare il campo **Chiamate** per visualizzare tutte le chiamate effettuate dal contatto bloccato.
  - ↳ A questo punto, è possibile eliminare le chiamate singolarmente o tutte allo stesso tempo.

  Toccare **Seleziona tutto** per selezionare l'intera cronologia delle chiamate da eliminare o apporre un segno di spunta accanto alle singole chiamate.

  Toccare **Elimina** per rimuovere queste chiamate oppure toccare **Indietro** per arrestare il processo di eliminazione.

  - ↳ All'utente viene richiesto di confermare l'eliminazione delle chiamate bloccate.

  Toccare **Elimina** per eliminare dalla cronologia le chiamate selezionate.

Toccare **Annulla** per arrestare il processo di eliminazione.

Report

Nella sezione **Report** della scheda **Impostazioni** vengono visualizzate tutte le attività di Avira Free Android Security effettuate tramite la Console Web.

Le informazioni registrate sono elencate per data e ora.

Qui di seguito viene riportato un esempio delle informazioni fornite da un report.

Data	Ora	Messaggio
Martedì 7 agosto 2012	15:17	Informazioni sul dispositivo aggiornate correttamente
Martedì 7 agosto 2012	14:05	Dispositivo localizzato
Lunedì 13 agosto 2012	18:11	Dispositivo sbloccato correttamente

Impostazioni

La scheda Impostazioni consente di gestire il nome e il numero di telefono del dispositivo. Inoltre, nella sezione **Report** è possibile controllare tutte le attività di Avira Free Android Security effettuate tramite la Console Web.

- Nella barra di navigazione fare clic sul dispositivo che si desidera gestire.
- Inserire nel campo **Nome dispositivo** il nome del dispositivo.
- Inserire nel campo **Numero di telefono** il numero di telefono del dispositivo.
- Fare clic su **Salva modifiche** per salvare le impostazioni definite per il dispositivo.
  - ↳ Nella Console Web Android di Avira viene segnalato che le impostazioni sono state salvate correttamente.

Installazione e disinstallazione

Installazione e disinstallazione

Download e installazione

Scaricare l'app Avira Free Android Security direttamente da Google Play sul dispositivo e installarla. Al termine dell'installazione, all'utente verrà chiesto di registrare il dispositivo nella schermata di registrazione di Avira Free Android Security. A tal fine, è possibile utilizzare il proprio account Google oppure l'indirizzo e-mail di un altro provider. Per la registrazione è necessario disporre di una connessione Internet stabile.

- Sul dispositivo toccare **Apri** per aprire il modulo di registrazione.
- Inserire i dati di accesso del proprio account Google oppure un altro indirizzo e-mail.
- Per continuare, toccare **Accettare il contratto di licenza con l'utente finale (EULA) e continuare**.
  - ↳ Avira invierà quindi all'indirizzo e-mail indicato la conferma relativa al nuovo account Avira Free Android Security. Nell'e-mail di conferma sarà riportato un link che consentirà all'utente di impostare la password personale necessaria per il login alla Console Web Android.
- Fare clic sul link riportato nell'e-mail di conferma per inserire una password e attivare la Console Web Android.
  - ↳ A questo punto, la Console Web permette all'utente il controllo remoto dei dispositivi.

Per attivare il comando **Ripristino impostazioni predefinite**, da utilizzare per eliminare tutti i dati in caso di smarrimento o furto del dispositivo, durante l'installazione è necessario attivare l'opzione **Amministratore dispositivo**:

- Per attivare la funzione Amministratore dispositivo, toccare **Abilita**.
  - ↳ Viene visualizzata la finestra di dialogo **Abilita amministratore dispositivo**.
- Confermare l'attivazione della funzione **Amministratore dispositivo** toccando il pulsante **Abilita**.
  - ↳ Una volta attivata tale funzione, l'utente permette ad Avira Free Android Security di eliminare tutti i dati presenti sul dispositivo tramite l'opzione **Ripristino impostazioni predefinite**.

Se non si è certi di voler attivare la funzione Amministratore dispositivo durante l'installazione, è possibile attivare tale opzione di configurazione anche in un secondo momento. Eseguire la procedura indicata di seguito:

- Accedere ad Avira Free Android Security dal dispositivo.
- Toccare **Impostazioni**.
  - ↳ A questo punto, è possibile vedere se l'opzione **Cancella dati con ripristino impostazioni predefinite** è attiva o meno.

- Toccare **Impostazioni di eliminazione**.
  - ↳ Viene visualizzata la finestra di dialogo **Abilita amministratore dispositivo**.
- Toccare il pulsante **Abilita** nella sezione inferiore della finestra di dialogo.
- Confermare l'attivazione della funzione Amministratore dispositivo toccando nuovamente il pulsante **Abilita**.
  - ↳ A questo punto, è possibile vedere se la funzione **Cancella dati con ripristino impostazioni predefinite** è attiva o meno.

- **Nota**
  L'utente può attivare o disattivare la funzione **Amministratore dispositivo** in qualunque momento mediante l'app Avira Free Android Security sul proprio dispositivo. Selezionare **Impostazioni > Impostazioni di eliminazione > Cancella dati con ripristino impostazioni predefinite > Abilita/Disabilita**.

Installazione mediante PC

È possibile scaricare l'app Avira Free Android Security mediante PC.

- Accedere a Google Play dal proprio computer.
- Ricercare l'app Avira Free Android Security.
- Fare clic su **Installa** per effettuare il download dell'applicazione sul PC.
  - ↳ Per poter installare l'app, all'utente verrà chiesto di effettuare il login.
- Fare clic su **Accedi** per richiamare il proprio account Google.
- Inserire i propri dati di accesso.
- Fare clic su **OK** per effettuare il download dell'applicazione sul dispositivo selezionato.
  - ↳ L'app Avira Free Android Security viene scaricata su tale dispositivo.
- Fare clic su **OK** per chiudere la finestra di download.
  - ↳ L'utente verrà reindirizzato a Google Play, in cui il pulsante **Installato** indica che l'applicazione è già stata scaricata sul dispositivo.

Disinstallazione

Per disinstallare Avira Free Android Security, è necessario eseguire due passaggi: disinstallare l'app dal dispositivo ed eliminare il dispositivo dall'account della Console Web Android di Avira.

Nota
Assicurarsi di aver disattivato la funzione **Amministratore dispositivo** prima della disinstallazione di Avira Free Android Security.

Disinstallare Avira Free Android Security tramite la gestione delle applicazioni del dispositivo.

- Toccare l'app Avira Free Android Security e selezionare **Disinstalla**.
- Confermare la disinstallazione.

Eliminare il dispositivo dall'account Avira Free Android Security della Console Web.

- Accedere alla Console Web.
- Nella barra del titolo fare clic sul link **Account**.
- Passare a Gestione dispositivi e accedere al menu a discesa **Dispositivi disponibili**.
- Selezionare il dispositivo da cui si desidera eliminare l'app Avira Free Android Security.
- Fare clic su **Elimina dispositivo** per rimuovere il dispositivo dall'account.

Reinstallazione

Una volta disinstallati tutti i dispositivi, non è più possibile accedere alla Console Web Avira.

È possibile, tuttavia, installare nuovamente l'app Avira Free Android Security su un dispositivo utilizzando l'account e-mail precedente.

- Effettuare il login alla Console Web inserendo i dati di accesso precedenti.
- Una volta effettuato il login, l'utente potrà modificare la propria password accedendo alla sezione **Gestione password**.

  Selezionare **Account > Gestione password**, immettere la nuova password e confermarla.
- Se si dimentica la password, al momento del login fare clic sul link **Password dimenticata?**.
  - ↳ All'utente sarà richiesto di inviare il proprio indirizzo e-mail e riceverà quindi un link di ripristino tramite il quale potrà impostare una nuova password.

Creazione dell'account Android

Per tenere il proprio smartphone sempre sott'occhio e proteggere i dati personali con l'ausilio di molteplici funzioni remote tramite la Console Web, è necessario creare innanzitutto un account Avira Free Android Security. È possibile creare un account già prima di scaricare l'app sul proprio dispositivo.

- Accedere al Control Center del proprio prodotto Avira.
- Fare clic su **Control Center > Protezione mobile > Android Security**.
  ↳ Verrà visualizzata la pagina di download di Avira Free Android Security.
- Fare clic su **Esegui il download adesso**.
  ↳ Verrà visualizzata la pagina di Google Play con le applicazioni Android.

  Fare clic su **Installa**.

  ↳ All'utente verrà richiesto di accedere a Google per effettuare il download dell'applicazione Avira Free Android Security.

  Fare clic su **Accedi**.

  Inserire l'indirizzo e-mail e la password.

  Fare clic su **Accedi**.

  Selezionare il dispositivo su cui si desidera scaricare Avira Free Android Security.

  Fare clic su **Installa**.

  ↳ L'app viene scaricata sul dispositivo Android dell'utente.
- Accedere ad Avira Free Android Security dal dispositivo.

  Toccare **Attività iniziali**.

  ↳ Verrà visualizzata la schermata dell'account utente.

  Inserire i propri dati di accesso.

  Per continuare, toccare **Accetta EULA e continua**.

  ↳ Avira invierà quindi un'e-mail di conferma per il nuovo account. Nell'e-mail di conferma sarà riportato un link che consentirà all'utente di impostare la password personale necessaria per il login alla Console Web Android.

  Fare clic sul link riportato nell'e-mail di conferma per inserire una password e attivare la Console Web Android.

  ↳ A questo punto, la Console Web permette all'utente il controllo remoto del dispositivo tramite il seguente sito Web: https://android.avira.com

Creazione rapida dell'account Android

Per tenere il proprio smartphone sempre sott'occhio e proteggere i dati personali con l'ausilio di molteplici funzioni remote tramite la Console Web, è necessario creare innanzitutto un account Avira Free Android Security. È possibile creare un account già prima di scaricare l'app sul proprio dispositivo.

- Accedere al sito Web Avira Free Android Security.
  ↳ Viene visualizzato il link della pagina di download di Avira Free Android Security.
- Fare clic sul pulsante **Accedi subito**.

↳ Viene visualizzata la pagina di login.

- Inserire il proprio indirizzo e-mail di Google oppure un altro indirizzo e-mail a scelta.

  Fare clic su **Crea account**.

  ↳ Avira invierà quindi un'e-mail di conferma all'indirizzo indicato. Nell'e-mail di conferma sarà riportato un link che consentirà all'utente di accedere alla Console Web di Avira Free Android Security.

- Fare clic sul link riportato nell'e-mail di conferma.

  ↳ L'utente sarà reindirizzato alla Console Web di Avira Free Android Security.

  ↳ A questo punto, la Console Web permette all'utente il controllo remoto dei dispositivi tramite il sito https://android.avira.com

- **Nota**
  Se l'utente scarica l'app Avira Free Android Security sul proprio dispositivo dopo aver effettuato la registrazione alla Console Web, durante l'installazione dovrà assicurarsi di utilizzare gli stessi dati di accesso nella schermata **Account utente**.

Accesso all'account Android

- Fare clic su **Control Center > Protezione mobile > Android Security**.

  ↳ Verrà visualizzata la pagina di download di Avira Free Android Security.

- Fare clic su **Accedi**.

  ↳ Verrà visualizzata la pagina di login di Avira Free Android Security.

  Inserire l'indirizzo e-mail registrato e la password.

  Fare clic su **Accedi** per accedere alla Console Web e alle relative funzioni di controllo remoto.

10.7 Generale

10.7.1 Categorie di minacce

Selezione delle categorie estese delle minacce (le opzioni sono disponibili solo se la modalità esperto è attiva)

Il prodotto Avira protegge dai virus del computer. Inoltre, si ha la possibilità di effettuare una scansione differenziata in base alle seguenti categorie di minacce.

- Adware
- Adware/Spyware
- Applicazioni
- Software di controllo backdoor

- File con estensioni nascoste
- Programmi di selezione a pagamento
- Phishing
- Programmi che violano la privacy dell'utente
- Programmi ludici
- Giochi
- Software ingannevole
- Programmi zip runtime insoliti

Facendo clic sulla casella appropriata viene attivata (spuntata) o disattivata (non spuntata) la modalità selezionata.

Attiva tutti

Se l'opzione è attivata vengono attivate tutte le modalità.

Valori standard

Questo pulsante ripristina i valori standard predefiniti.

> **Nota**
> Se viene disattivata una modalità, i file riconosciuti come tale tipo di programma non verranno più segnalati. Non viene riportata alcuna segnalazione nemmeno sul file di report.

10.7.2 Password

Tutti i prodotti Avira possono essere protetti in diverse sezioni mediante una password. Se si inserisce una password questa verrà richiesta ogni volta che si desidera aprire una sezione protetta.

Password

Inserimento password

Inserire qui la password desiderata. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*). È possibile inserire un numero massimo di 20 caratteri. Se è stata inserita una password, il programma negherà l'accesso in caso di inserimento di password errata. Un campo vuoto equivale a "Nessuna password".

Conferma

Inserire nuovamente la password per conferma. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

> **Nota**
> Attenzione alle lettere maiuscole o minuscole!

Aree protette da password (le opzioni sono disponibili solo se la modalità esperto è attiva).

Il prodotto Avira consente di proteggere con password ogni singola sezione. Facendo clic sulla casella appropriata, la richiesta di password per alcune sezioni può essere disattivata o riattivata.

Sezione protetta da password	Funzione
Control Center	Se l'opzione è attivata, per l'avvio del Control Center è necessaria la password impostata.
Attiva/disattiva Real-Time Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Real-Time Protection di Avira è necessario inserire la password impostata.
Attiva/disattiva Web Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Web Protection è necessario inserire la password impostata.
Quarantena	Se l'opzione è attivata,
Ripristina gli oggetti infetti	Se l'opzione è attivata, per il ripristino degli oggetti è necessario inserire la password impostata.
Nuovo controllo di oggetti infetti	Se l'opzione è attivata, per il nuovo controllo degli oggetti è necessario inserire la password impostata.
Apri gli oggetti infetti	Se l'opzione è attivata, per la visualizzazione delle proprietà degli oggetti è necessario inserire la password impostata.
Elimina gli oggetti infetti	Se l'opzione è attivata, per l'eliminazione degli oggetti è necessario inserire la password impostata.

Invia e-mail ad Avira	Se l'opzione è attivata, per l'invio degli oggetti al Malware Research Center Avira è necessario inserire la password impostata.
Aggiungi e modifica job	Se l'opzione è attivata, per aggiungere e modificare job nel pianificatore è necessario inserire la password impostata.
Configurazione	Se l'opzione è attivata, è possibile configurare il programma solo dopo l'inserimento della password impostata.
Installazione/Disinstallazione	Se l'opzione è attivata, per installare o disinstallare il programma è necessaria la password impostata.

10.7.3 Sicurezza

Le opzioni sono disponibili solo se la modalità esperto è attiva.

Esecuzione automatica

Blocca esecuzione automatica

Se l'opzione è attivata, la funzione di esecuzione automatica di Windows viene bloccata su tutti i drive collegati, come penne USB, CD e DVD, drive di rete. Con la funzione di esecuzione automatica di Windows, i file sui supporti informatici o sui drive di rete vengono letti immediatamente al momento dell'inserimento o del collegamento; in questo modo i file possono essere avviati e riprodotti automaticamente. Tuttavia questa funzionalità nasconde un rischio per la sicurezza molto elevato, poiché con l'avvio automatico dei file è possibile che vengano installati malware e programmi indesiderati. La funzione di esecuzione automatica è particolarmente critica nel caso delle penne USB poiché su questi supporti i file possono modificarsi continuamente.

Escludi CD e DVD

Se l'opzione è attivata, la funzione di esecuzione automatica è consentita su CD e DVD.

Attenzione
Disattivare la funzione di esecuzione automatica per CD e DVD solo se si è sicuri che si tratti di supporti informatici assolutamente affidabili.

Protezione del sistema

Proteggi il file host di Windows da modifiche

Se l'opzione è attivata, il file host di Windows è disponibile in sola lettura. Non è più possibile manipolare il file. Il malware non è più, ad esempio, in grado di deviare l'utente su pagine Internet indesiderate. Questa opzione è attivata di default.

Tutela del prodotto

> **Nota**
> Se durante l'installazione personalizzata si è deciso di non installare Real-Time Protection, le opzioni di tutela del prodotto non saranno disponibili.

Proteggi i processi da una chiusura indesiderata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata dovuta a virus e malware o da chiusura involontaria di un utente, ad esempio mediante Task Manager. Questa opzione è attivata di default.

Protezione del processo avanzata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata con metodi avanzati. La protezione avanzata del processo consuma molte più risorse rispetto alla protezione di processo base. L'opzione è attivata di default. Per disattivare l'opzione è necessario riavviare il computer.

> **Nota**
> La protezione del processo in Windows XP a 64 bit non è disponibile.

> **Attenzione**
> Se la protezione del processo è attivata, possono verificarsi problemi di interazione con altri software. In tal caso disattivare la protezione del processo.

Proteggi i file e le voci di registrazione dalla manipolazione

Se l'opzione è attivata, tutte le voci di registro del programma e tutti i dati del programma (file binari e di configurazione) vengono protetti da manipolazione. La protezione da manipolazione comprende la protezione da interventi di scrittura, eliminazione e talvolta di lettura sulle voci del registro o sui file di programma da parte di utenti o di programmi estranei. Per attivare l'opzione è necessario riavviare il computer.

> **Attenzione**
> Tenere presente che, se l'opzione è disattivata, è possibile che la riparazione di computer infetti a causa di determinati tipi di malware non possa essere effettuata.

> **Nota**
> Se l'opzione è attivata, è possibile apportare modifiche alla configurazione oppure a job di scansione e aggiornamento solo tramite l'interfaccia utente.

> **Nota**
> La protezione dei file e delle voci di registrazione in Windows XP a 64 bit non è disponibile.

10.7.4 WMI

Le opzioni sono disponibili solo se la modalità esperto è attiva.

Assistenza per Windows Management Instrumentation (WMI)

Windows Management Instrumentation è una tecnologia di gestione fondamentale di Windows che consente, mediante linguaggi di script e di programmazione in lettura e in scrittura, di accedere in locale e in remoto alle impostazioni dei computer Windows. Il prodotto Avira supporta WMI e rende disponibili dati (informazioni di stato, dati statistici, report, job pianificati ecc.), eventi in un'interfaccia. Tramite WMI è possibile richiamare dati operativi del programma.

Attiva assistenza WMI

Se l'opzione è attivata, è possibile richiamare i dati operativi del programma tramite WMI.

10.7.5 Eventi

Le opzioni sono disponibili solo se la modalità esperto è attiva.

Limitare l'estensione della banca dati degli eventi

Limita l'estensione ad un massimo di n immissioni

Se l'opzione è attiva, il numero massimo delle immissioni nella banca dati degli eventi è limitato a un preciso numero; i valori consentiti sono: da 100 a 10.000 immissioni. Se il numero delle immissioni viene superato, gli inserimenti più vecchi vengono eliminati.

Elimina tutti gli eventi più vecchi di n giorno/i

Se l'opzione è attiva, dopo un numero determinato di giorni gli eventi vengono eliminati dalla banca dati degli eventi; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Se l'opzione è attivata, le dimensioni della banca dati degli eventi non sono limitate. Sull'interfaccia del programma, alla voce Eventi, viene però visualizzato un massimo di 20.000 immissioni.

10.7.6 Report

Le opzioni sono disponibili solo se la modalità esperto è attiva.

Limita i report

Limita il numero a un massimo di n pezzi

Se l'opzione è attiva, il numero massimo di report può essere limitato a un determinato numero; i valori consentiti sono: da 1 a 300. Se il numero indicato viene superato, i report più vecchi vengono eliminati.

Elimina tutti i report più vecchi di n giorni

Se l'opzione è attiva, i report vengono automaticamente eliminati dopo un determinato numero di giorni; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Se l'opzione è attiva il numero di report non è limitato.

10.7.7 Directory

Le opzioni sono disponibili solo se la modalità esperto è attiva.

Percorso temporaneo

Utilizza le impostazioni predefinite

Se l'opzione è attivata vengono utilizzate le impostazioni del sistema per la gestione dei file temporanei.

> **Nota**
> Per sapere dove vengono salvati i file temporanei, ad esempio in Windows XP, accedere a: **Start > Impostazioni > Pannello di controllo > Sistema >** scheda "**Avanzate**" > pulsante "**Variabili d'ambiente**". Le variabili temporanee (`TEMP`, `TMP`) per l'utente di volta in volta registrato e per le variabili di sistema (`TEMP`, `TMP`) sono visibili qui con i loro rispettivi valori.

Utilizza la seguente directory

Se l'opzione è attivata viene utilizzato il percorso visualizzato nel campo.

Campo

In questo campo è possibile immettere il percorso in cui si desidera che vengano salvati i file temporanei del programma.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il percorso temporaneo desiderato.

Standard

Il pulsante crea la directory predefinita per il percorso temporaneo.

10.7.8 Avviso acustico

Le opzioni sono disponibili solo se la modalità esperto è attiva.

In caso di rilevamento di un virus o di malware tramite System Scanner o Real-Time Protection, viene emesso un avviso acustico in modalità di azione interattiva. È possibile attivare o disattivare l'avviso acustico nonché selezionare un file WAVE alternativo come avviso acustico.

> **Nota**
> La modalità di azione di System Scanner viene impostata nella configurazione in Sicurezza del computer > System Scanner > Scansione > Azione in caso di rilevamento.

Nessun avviso

Se l'opzione è attivata, non viene emesso alcun avviso acustico in caso di rilevamento di un virus tramite System Scanner o Real-Time Protection.

Emetti tramite casse PC (solo in modalità interattiva)

Se l'opzione è attivata, viene emesso un avviso acustico con suono standard in caso di rilevamento di un virus tramite System Scanner o Real-Time Protection. L'avviso acustico viene emesso tramite l'altoparlante interno del PC.

Utilizza il seguente file WAVE (solo in modalità interattiva)

Se l'opzione è attivata, in caso di rilevamento di un virus tramite System Scanner o Real-Time Protection, viene emesso un avviso acustico con il file WAVE selezionato. Il file WAVE selezionato viene riprodotto tramite un altoparlante collegato esternamente.

File WAVE

In questo campo è possibile inserire il nome e il percorso corrispondente di un file audio a scelta. L'avviso acustico standard del programma è registrato come impostazione predefinita.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file desiderato tramite Esplora file.

Test

Questo pulsante serve a testare il file WAVE selezionato.

10.7.9 Avvisi

In caso di determinati eventi, il prodotto Avira genera notifiche sul desktop, i cosiddetti messaggi a tendina, per informare l'utente di eventuali pericoli o della riuscita o meno dell'esecuzione di un dato programma come, per esempio, un aggiornamento. È possibile attivare o disattivare in **Avvisi** la funzione di notifica per specifici eventi.

Nel caso delle notifiche sul desktop è possibile disattivare direttamente le notifiche sul messaggio a tendina. È possibile annullare la disattivazione della notifica nella finestra di configurazione **Avvisi**.

Aggiornamento

Avviso se l'aggiornamento risale a più di n giorni fa

In questo campo è possibile inserire il numero massimo di giorni che possono trascorrere dall'ultimo aggiornamento. Superato questo intervallo di tempo, il Control Center visualizzerà sotto Stato un'icona rossa per lo stato dell'aggiornamento.

Avvisa se il file VDF non è aggiornato

Se l'opzione è attivata, si riceve un avviso in caso di file di definizione dei virus non aggiornato. Grazie all'opzione "Avviso se l'aggiornamento risale a più di n giorni fa", è possibile configurare un intervallo temporale.

Avvisi/indicazione nelle seguenti situazioni

Utilizzo di una connessione dial-up

Se l'opzione è attivata, l'utente è avvisato con una notifica sul desktop quando un programma di selezione stabilisce una connessione sul computer tramite la rete telefonica o ISDN. In caso di programmi di selezione esiste il rischio che si tratti di un dialer sconosciuto e indesiderato che stabilisce una connessione a pagamento (vedere Categorie di minacce: programma di selezione a pagamento).

File aggiornati correttamente

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato completato con successo un aggiornamento e sono stati aggiornati file.

Aggiornamento non riuscito

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando l'aggiornamento non riesce, il che significa che non è stato possibile stabilire una

connessione con il server di download oppure non è stato possibile installare i file di aggiornamento.

Non sono necessari aggiornamenti

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando viene lanciato un aggiornamento ma non è necessario installare alcun file perché il programma è già aggiornato.